

Gesetzentwurf

der Staatsregierung

Gesetz zur Änderung polizeirechtlicher Vorschriften

Vorblatt

zum Entwurf eines Gesetzes zur Änderung polizeirechtlicher Vorschriften

A. Zielstellung

Das Gesetzesvorhaben dient der Umsetzung höchstrichterlicher Rechtsprechung (Sächsischer Verfassungsgerichtshof und Bundesverfassungsgericht). Änderungsbedarf folgt zudem aus dem Koalitionsvertrag 2024 bis 2029, ferner im Hinblick auf EU-Recht und den polizeifachlichen Bedarf nach zeitgemäßen und modernen Befugnissen.

B. Wesentlicher Inhalt

Seit der letzten grundlegenden Novellierung des Polizeirechts durch das Gesetz zur Neustrukturierung des Polizeirechts des Freistaates Sachsen vom 11. Mai 2019 hat sich umfangreicher Ergänzungs- und Änderungsbedarf beim Sächsischen Polizeivollzugsdienstgesetz ergeben. Dieser folgt zum einen aus höchstrichterlicher Rechtsprechung, aus dem sicherheitspolitischen Erfordernis, auch künftig effektive vorbeugende Kriminalitätsbekämpfung gewährleisten zu können und aus dem Koalitionsvertrag 2024 bis 2029 zwischen CDU und SPD vom 4. Dezember 2024.

Der Gesetzentwurf setzt die Vorgaben des Sächsischen Verfassungsgerichtshofs (Urteil vom 25. Januar 2024, Vf. 91-II-19) an die verfassungsrechtliche Ausgestaltung der Eingriffsschwellen bei verdeckten Überwachungsmaßnahmen und an Befugnisregelungen zur Weiterverarbeitung von in Informationssystemen der Polizei vorsorgend gespeicherten personenbezogenen Daten um.

Im Sächsischen Polizeivollzugsdienstgesetz werden ferner u. a. Vorgaben des Bundesverfassungsgerichts aus:

- dem Grundsatz-Urteil vom 1. Oktober 2024, 1 BvR 1160/19 (Bundeskriminalamtsgesetz II), zur Ausgestaltung der gesetzlichen Regelungen zur „vorsorgenden Speicherung“ von personenbezogenen Daten,
- dem Beschluss vom 27. Mai 2020, 1 BvR 1873/13, 1 BvR 2618/13 (Bestandsdatenauskunft II), zu den Anforderungen an die Ausgestaltung der Auskunft über Bestandsdaten von Telekommunikationsdiensten und der Rechtsprechung zum „Doppeltürmodell“ sowie
- dem Beschluss vom 9. Dezember 2022, 1 BvR 1345/21, zur Stärkung des Kernbereichsschutzes auf der Erhebungs-, Auswertungs- und Verarbeitungs- oder Verwendungsebene beim Einsatz von verdeckten Ermittlerinnen, verdeckten Ermittlern und V-Personen

umgesetzt.

Um eine effektive vorbeugende Kriminalitätsbekämpfung auch künftig gewährleisten zu können, werden folgende neue Befugnisse für den Polizeivollzugsdienst geschaffen:

- Abwehr von „Drohnen“,
- „intelligente Videoüberwachung“ bis hin zu biometrischer Echtzeit-Fernidentifizierung,
- anlassbezogene automatisierte Datenanalyse mittels regelbasierter oder selbstlernender Systeme,
- anlassbezogener biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet,
- Trainingsbefugnis für regelbasierte und lernende IT-Systeme.

Im Hinblick auf die anlassbezogene automatisierte Datenanalyse (§ 62a) werden zu den zum gegenwärtigen Zeitpunkt bestehenden Rahmenbedingungen vertragliche Vereinbarungen des Freistaates Sachsen mit der Firma Palantir ausgeschlossen. Mit der Aufnahme der neuen Befugnisregelung der anlassbezogenen automatisierten Datenanalyse ist keine Festlegung auf ein bestimmtes IT-System verbunden.

In Umsetzung von Regelungs- und Prüfaufträgen des Koalitionsvertrags erfolgt die Aufnahme von Rechtsgrundlagen für:

- die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) zur Abwehr von Gefahren für überragend wichtige Rechtsgüter oder zur Abwehr terroristischer Straftaten,
- die Verbesserung des Schutzes von Opfern und potentiellen Opfern häuslicher Gewalt,
- die Erweiterung des Einsatzes von Bodycams auf den Bereich von Wohnungen.

Die Neufassung des Polizeirechtes bedingt einen redaktionellen Anpassungsbedarf in anderen Gesetzen.

C. Alternativen

Im Sinne der Zielsetzung keine, insbesondere können die Regelungsziele nicht durch untergesetzliche Maßgaben erreicht werden.

D. Folgewirkungen und Kosten

I. Ergebnis des Demografietests

Zwischen dem Vorhaben und der Bevölkerungsentwicklung besteht keine Wirkungsbeziehung.

II. Ergebnis der Prüfung der Möglichkeit der vollständigen oder teilweisen Digitalisierung (Nummer 5 der Anlage 1 [zu Nummer 2] zur VwV Normerlass)

Die Umsetzung der Vorschriften zur Datenverarbeitung soll vollständig digitalisiert erfolgen.

III. Haushaltsauswirkungen ohne Erfüllungsaufwand (vgl. Kostenblatt)

Das Gesetzesvorhaben hat finanzielle Mehraufwendungen für den Landeshaushalt zur Folge. Die Mehraufwendungen für die Haushaltsjahre 2026 bis 2029 werden auf insgesamt 7,005 Mio. EUR geschätzt. Ergänzend wird auf das beigefügte Kostenblatt verwiesen.

IV. Darstellung des Erfüllungsaufwandes, sofern ein Prüfungsrecht des Sächsischen Normenkontrollrates besteht (andernfalls Begründung, warum das Prüfungsrecht entfällt)

1. Erfüllungsaufwand für Bürgerinnen und Bürger

Das Gesetz bewirkt keinen Erfüllungsaufwand bei Bürgerinnen und Bürgern.

2. Erfüllungsaufwand für die Wirtschaft

Das Gesetz bewirkt keinen Erfüllungsaufwand bei der Wirtschaft.

3. Erfüllungsaufwand für die Verwaltung

a) Polizeivollzugsdienst

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

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

b) Polizeibehörden

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

Die Änderungen im Sächsischen Polizeibehördengesetz bedingen keinen Erfüllungsaufwand.

c) Sächsische Datenschutz- und Transparenzbeauftragte

Die neuen oder ergänzten Befugnisregelungen in den § 57a Absatz 1 Satz 4 und Absatz 2, § 58, § 60, § 61, § 62a, § 62b, § 66 Absatz 2 sowie § 79c führen zu einer Erweiterung von Aufgaben der Sächsischen Datenschutz- und Transparenzbeauftragten; dies gilt sowohl hinsichtlich zusätzlicher Kontrollen gemäß § 94 SächsPVDG als auch hinsichtlich des neu eingeführten Abstimmungs- und Informationsaufwands im Zusammenhang mit dem Erlass von geplanten Verwaltungsvorschriften in § 57a Absatz 7, § 62b Absatz 8 und 79c Absatz 6 SächsPVDG-E. Der zusätzliche Zeitaufwand für die gesetzeskonforme Prüfung wird durch die Sächsische Datenschutz- und Transparenzbeauftragte mit ca. 565 Stunden geschätzt. Hierfür wird ein Stellenmehrbedarf von 0,25 VZÄ verursacht.

d) Justiz

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

- Datenweiterverarbeitung von durch Bodycam-Einsatz in Wohnungen erlangten Daten (§ 57 Absatz 8 Satz 6),
- besondere Datenverarbeitungsbefugnis im Hinblick auf Daten aus einer Videoüberwachung (§ 57a Absatz 5 Satz 1),

- Verlängerung der Ausschreibung zur verdeckten Beobachtung (§ 60 Absatz 3 Satz 2),
- anlassbezogene automatisierte Datenanalyse unter Anwendung selbstlernender Systeme (§ 62a Absatz 8 Satz 3),
- Erstellung eines Verhaltensprofils mittels automatisierter Datenanalyse (§ 62a Absatz 8 Satz 5),
- biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet (§ 62b Absatz 3 Satz 1),
- Quellen-TKÜ (§§ 66 Absatz 4 Satz 1)

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

V. Weitere Wirkungen, insbesondere sonstige Kosten für die Wirtschaft oder soziale Sicherungssysteme sowie Auswirkungen auf Einzelpreise und das Preisniveau

Keine.

E. Ergebnis der Prüfung zum Mehrbelastungsausgleich nach Artikel 85 Abs. 2 SächsVerf

Entfällt.

F. Gleichstellungspolitische Relevanz

Entfällt

G. Zuständigkeit

Das Sächsische Staatsministerium des Innern ist zuständig.

Kostenblatt zum

Entwurf eines Gesetzes zur Änderung polizeirechtlicher Vorschriften

Übersicht über die Auswirkungen

I. Auswirkungen auf den Landeshaushalt/mittelfristige Finanzplanung

Kosten der vorgeschlagenen Maßnahme und damit verbundene Einnahmen - in TEUR -
1:

Haushalts-/Planungsjahr	Ausgaben		Einnahmen	
	insgesamt	davon bereits im Haushalt / in der Mipla enthalten	insgesamt	davon bereits im Haushalt / in der Mipla enthalten
2026	888,5	0	0	0
2027	914,0	150,0	0	0
2028	1.929,0	150,0	0	0
2029	3.274,0	0	0	0

II. Auswirkungen auf die Haushalte der Gemeinden, Landkreise und kreisfreien Städte - in TEUR -¹:

	Gemeinden		Landkreise		Kreisfreie Städte	
	Ausgaben	Einnahmen	Ausgaben	Einnahmen	Ausgaben	Einnahmen
2026		0		0		0
2027		0		0		0
2028		0		0		0
2029		0		0		0

¹ fallen keine Kosten an, erfolgt in allen Feldern der Eintrag „0“

III. Stellen

Für die vorgeschlagenen Maßnahmen sind folgende Stellen erforderlich²:

2026	2027	2028	2029
0	0	0	0

davon bereits im Haushalt oder in der Mipla enthalten²:

2026	2027	2028	2029
0	0	0	0

IV. Bemerkungen

Das Inkrafttreten des Gesetzes muss bis zum 30. Juni 2026 erfolgen, anderenfalls treten die durch den Sächsischen Verfassungsgerichtshof für verfassungswidrig erklärten Bestimmungen außer Kraft. Eine umfassende Darstellung der Auswirkungen des Gesetzentwurfs auf den Haushalt kann nicht erfolgen.

Die der Landespolizei entstehenden Kosten für Befugnisenerweiterungen oder neue Befugnisse lösen nicht unmittelbar haushälterische Auswirkungen aus, sondern bedingen eine lage- und erforderlichkeitsbedingte Anschaffungspriorisierung. Der Mittelbedarf kann aktuell sowohl hinsichtlich des Umfangs, als auch im Hinblick auf die zeitliche Einordnung nur grob geschätzt werden. Für die Beschaffung beispielsweise von Software zur Umsetzung der Befugnis nach § 62a, anlassbezogene automatisierte Datenanalyse, ist bei einer zentralen Bereitstellung durch den Bund und einer Kostenverteilung nach dem Königsteiner-Schlüssel für Sachsen mit Kosten in einer Höhe von jährlich ca. 2,5 Mio. EUR auszugehen. Die erforderlichen Haushaltsmittel werden jedoch voraussichtlich erst nach 2028 haushaltswirksam.

Der Gesetzentwurf löst unmittelbare Kosten für die Durchführung einer externen Evaluierung zu den neuen Befugnisnormen in §§ 21 Abs. 6, 40 Abs. 5, 57 Abs. 10, 58 Abs. 6, 61 Abs. 7 und in § 66 Abs. 6 (aufgrund Koalitionsvertrags) in einer voraussichtlichen Gesamthöhe zwischen mindestens 180.000 und 300.000 EUR in 2027 (Abschlagszahlung) und in 2028 oder 2029/2030 (Restzahlung) aus.

Die voraussichtlichen finanziellen Auswirkungen auf den Landeshaushalt sind, soweit bezifferbar, derzeit weder im Haushaltsplan 2025/2026 noch in der mittelfristigen Finanzplanung – bis auf einen Betrag von insgesamt 300,0 TEUR für den Einsatz von unbemannten Luftfahrtsystemen (§ 71) – enthalten und bleiben daher dem weiteren Gesetzgebungsverfahren, insbesondere der Beschlussfassung durch den Sächsischen Landtag, vorbehalten (Haushaltsvorbehalt). Mögliche Mehrausgaben im Haushaltsjahr 2026 werden im Rahmen der im Doppelhaushalt 2025/2026 veranschlagten Ansätze des Epl. 03 verausgabt.

² sind keine zusätzlichen Stellen erforderlich, erfolgt in allen Feldern der Eintrag „0“

Gesetz zur Änderung polizeirechtlicher Vorschriften

Vom ...

Der Sächsische Landtag hat am ... 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 folgende Angabe eingefügt:

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

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

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

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

„§ 57a Anwendungen zur automatisierten Verarbeitung von an öffentlichen Orten und besonders gefährdeten öffentlichen Einrichtungen offen erhobenen personenbezogenen Daten, 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 § 64 wird folgende Angabe eingefügt:

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

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

„§ 66a Unterbrechung oder Verhinderung der Telekommunikation“.

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

„§ 69 (weggefallen)“.

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

„§ 71 Einsatz von unbemannten Luftfahrtssystemen“.

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

„§ 72 (weggefallen)“.

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

„§ 79 Befugnis zur Datenverarbeitung“.

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

„§ 79a Zweckbindung, Zweckänderung, Hypothetische Datenneuerhebung

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

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

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

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

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

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

§ 80b Vorsorgende Speicherung von zu Gefahrenabwehrzwecken erhobenen Daten

§ 80c Vorsorgende Speicherung von personenbezogenen Daten zu sonstigen Personen

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

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

„§ 84a Öffentlichkeitsfahndung“.

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

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

s) Nach der Angabe zu § 88 wird folgende Angabe eingefügt:

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

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

„§ 106a Ordnungswidrigkeiten“.

2. § 3 wird durch folgenden § 3 ersetzt:

„§ 3

Tätigwerden der Polizei für die Polizeibehörden oder andere Stellen

Wird die Polizei gemäß § 2 Absatz 3 tätig, trifft sie die erforderlichen 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 folgende Nummern 5 bis 9 ersetzt:

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

a) die Bevölkerung auf erhebliche Weise einzuschüchtern,

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

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

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

6. Vorfeldstraftat: Straftatbestand, der Verhaltensweisen erfasst, die in räumlicher oder zeitlicher Hinsicht noch vor einer konkreten oder konkretisierten Gefährdung oder Verletzung der geschützten Individualrechtsgüter oder Kollektivrechtsgüter liegen können und entweder aufgrund ihrer abstrakten Gefährlichkeit oder als Vorbereitungshandlungen unter Strafe gestellt sind; soweit dieses Gesetz Maßnahmen zur Verhinderung von Vorfeldstraftaten davon abhängig macht, dass im Einzelfall tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen, gilt, dass als Rechtsgut in diesem Sinne nur Individualrechtsgüter oder Kollektivrechtsgüter in Betracht kommen, die ihrer Natur nach einer konkreten Gefährdung zugänglich sind, und dass unklare und unabgrenzbare Schutzrichtungen nicht genügen;
 7. Ordnungswidrigkeiten von erheblicher Bedeutung: Ordnungswidrigkeiten, bei deren Begehung ein Schaden für ein bedeutsames Rechtsgut, wie Bestand oder Sicherheit des Bundes oder eines Landes, Leben, Gesundheit, Freiheit einer Person oder bedeutende Sach- und Vermögenswerte, zu befürchten ist oder wenn die Vorschrift ein sonst bedeutsames Interesse der Allgemeinheit schützt;
 8. 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 7 wird durch folgende Nummern 7 und 8 ersetzt:
- „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 Satz 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 Mit-

tel 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 folgende 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 14. Tages nach ihrer Anordnung, soweit nicht die Polizei im Einzelfall eine kürzere Frist festlegt. Stellt die gefährdete Person während der nach Satz 3 bestimmten Dauer der Maßnahmen einen Antrag nach dem Gewaltschutzgesetz, enden die Maßnahmen mit dem Tag der gerichtlichen Entscheidung oder des gerichtlichen Vergleichs, spätestens jedoch mit Ablauf des 14. Kalendertages nach dem Ende der nach Satz 3 bestimmten Dauer.

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

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 Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen. Unter den Voraussetzungen der Sätze 1 und 2 kann die Polizei auch den Kontakt mit bestimmten Personen oder Personen einer bestimmten Gruppe untersagen, wenn Tatsachen die Annahme rechtfertigen, dass diese von der Vorbereitung der drohenden Straftat Kenntnis haben, diese aus der Tat Vorteile ziehen werden oder die Person sich ihrer zur Begehung bedienen wird (Kontaktverbot). Anordnungen

nach den Sätzen 1 bis 3 sind auf höchstens zwei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als zwei Monate ist zulässig, soweit die Voraussetzungen weiterhin vorliegen. Für Maßnahmen nach Absatz 2 gilt im Übrigen Absatz 1 Satz 2 und 3.

(3) Maßnahmen nach Absatz 2 bedürfen der Anordnung durch das Amtsgericht auf 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 Be dienstete 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 folgende Nummern 6 bis 8 ersetzt:

- „6. es sich um ein Land-, Wasser- oder Luftfahrzeug handelt, in dem sich eine Person befindet, deren Identität nach § 15 Absatz 1 Satz 1 Nummer 4, 6 oder 7 festgestellt werden darf oder die zur gezielten Kontrolle ausgeschrieben ist; die Durchsuchung kann sich auch auf die in diesem Fahrzeug enthaltenen oder mit dem Fahrzeug verbundenen Sachen erstrecken,
 7. sie von einer Person mitgeführt wird, deren Identität nach § 15 Absatz 1 Satz 1 Nummer 4, 5, 6 oder 7 festgestellt werden darf, oder
 8. es sich um ein Fahrzeug handelt, das zur gezielten Kontrolle ausgeschrieben ist und tatsächliche Anhaltspunkte dafür vorliegen, dass die Durchsuchung zur Abwehr einer Gefahr erforderlich ist“.
10. § 29 Absatz 3 wird durch folgenden Absatz 3 ersetzt:
- „(3) Während der Nachtzeit (§ 104 Absatz 3 der Strafprozessordnung) darf eine Wohnung nur in den Fällen des Absatzes 1 Satz 1 Nummer 2 betreten und durchsucht werden. Diese Einschränkung gilt nicht, wenn von der Wohnung eine erhebliche, die Gesundheit Dritter beeinträchtigende Störung ausgeht.“
11. § 40 wird wie folgt geändert:
- a) In Absatz 4 Satz 2 wird die Angabe „von Spezialeinheiten“ gestrichen.
 - b) Nach Absatz 4 wird der folgende Absatz 5 eingefügt:

„(5) Die Erforderlichkeit, die praktische Anwendung und die Auswirkungen des Einsatzes von Vorrichtungen für den Abschuss besonderer Formen von Projektilen durch Polizeibedienstete, die außerhalb von Spezialeinheiten zum Einsatz kommen, werden nach einem Erfahrungszeitraum von drei Jahren, spätestens jedoch zum 31. Dezember 2029 von der Staatsregierung geprüft. Die Staatsregierung berichtet dem Landtag über das Ergebnis der Evaluierung.“
12. § 41 wird wie folgt geändert:
- a) Absatz 1 Satz 3 wird durch folgenden Satz 3 ersetzt:

„Das angewendete Mittel muss nach Art und Maß den jeweiligen Umständen, insbesondere dem Verhalten, dem Alter und dem Zustand der oder des Betroffenen angemessen sein.“
 - b) Absatz 2 wird durch 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 gelten 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.“
13. In § 48 Absatz 3 Satz 2 wird die Angabe „Erwerbstätigkeit“ durch die Angabe „Erwerbsfähigkeit“ ersetzt.

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

„§ 57

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

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

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

(3) Die Polizei kann

1. an oder in den Objekten im Sinne des § 15 Absatz 1 Satz 1 Nummer 3 oder in deren unmittelbarer Nähe und
2. auf öffentlichen Straßen, Wegen oder Plätzen, wenn nach polizeilich dokumentierten Tatsachen die Kriminalitätsbelastung dort gegenüber der des Gemeindegebiets deutlich erhöht ist (Kriminalitätsschwerpunkte),

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

(4) Die Polizei kann zur Gefahrenabwehr durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen personenbezogene Daten kurzzeitig in einem Zwischenspeicher für 60 Sekunden erfassen, soweit und solange dies mit hinreichender Wahrscheinlichkeit zum Schutz der eigenen oder einer dritten Person gegen eine Gefahr für Leib oder Leben erforderlich ist. In Wohnungen ist eine Maßnahme nach Satz 1 nur zulässig, wenn dies 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 Berufsgeheimnisträgern nach den §§ 53 und 53a der Strafprozessordnung dienen, sind Maßnahmen nach Absatz 4 und 5 unzulässig. Ergeben sich während der Durchführung einer Maßnahme nach Absatz 5 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 evaluiert. Die Staatsregierung berichtet dem Landtag über das Ergebnis der Evaluierung.

(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 unbedingt erforderlich ist.

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

1. zur Abwehr einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr durch die Begehung einer terroristischen Straftat, soweit es die Daten der Personen betrifft, die diese Gefahr verursachen, oder
2. zur Suche nach im Datenbestand der polizeilichen Auskunfts- und Fahndungssysteme gespeicherten
 - a) Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung oder
 - b) vermissten Personen.

Soweit es sich bei der terroristischen Straftat um eine Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen.

(3) Maßnahmen nach Absatz 1 Satz 1, 3 und 4 sowie Absatz 2 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 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. § 79a findet keine Anwendung. 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 spurlos 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) Das Staatsministerium des Innern 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 begangen werden sollen.

Maßnahmen nach § 60 sind unzulässig.

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

1. nach § 60 oder einer vergleichbaren Vorschrift eines anderen Landes, den §§ 163e und 463a der Strafprozessordnung, Artikel 36 der Verordnung (EU) 2018/1862 und § 47 des Bundeskriminalamtgesetzes,
2. auf Grund einer Gefahr für Zwecke der Gefahrenabwehr,
3. auf Grund des Verdachts einer Straftat für Zwecke der Strafverfolgung oder
4. aus Gründen der Strafvollstreckung

in den Sachfahndungsbeständen der Informationssysteme der Polizei und im Schengener Informationssystem ausgeschrieben sind. In den Fällen des Absatzes 1 Nummer 1 darf ein Abgleich nur mit den zu diesen Zwecken gespeicherten personenbezogenen Daten erfolgen. Im Übrigen sind die einzubeziehenden Fahndungsbestände auf

solche Kennzeichendaten zu beschränken, die für die jeweiligen Zwecke Bedeutung haben können. Der Abgleich darf nur mit vollständigen erfassten Kennzeichen des Fahndungsbestandes erfolgen.

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

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

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

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

15. § 59 wird gestrichen.

16. 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 Straftat um eine Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen.

(2) Wird eine nach Absatz 1 ausgeschriebene Person, 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 angetroffene Personen oder Insassen des Fahrzeugs und mitgeführte Sachen,
2. im Fall der gezielten Kontrolle, zusätzlich zu den Erkenntnissen nach Nummer 1, solche aus § 27 Absatz 1 Nummer 6 und § 28 Absatz 1 Nummer 6 bis 8 sowie
3. im Fall der Ermittlungsanfrage die durch die Befragung der Person erlangten Erkenntnisse.

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

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

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift,
2. Art, Umfang und Dauer der Maßnahme,
3. der Sachverhalt sowie
4. die Begründung.

§ 61

Elektronische Aufenthaltsüberwachung

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

1. dies zum Schutz einer bestimmten anderen gefährdeten Person erforderlich ist, weil Tatsachen die Annahme rechtfertigen, dass dann, wenn die überwachte Person bestimmte Orte betritt, aufsucht oder sich dort aufhält oder mit der gefährdeten Person zusammentrifft, Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung, soweit sie durch Straftatbestände geschützt ist, die im Mindestmaß mit wenigstens drei Monaten Freiheitsstrafe bedroht sind, der gefährdeten Person innerhalb eines absehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise durch einen Angriff von erheblicher Intensität oder Auswirkung gefährdet sind,
2. gegen die Person eine Maßnahme nach § 21 Absatz 2 angeordnet wird und Tatsachen die Annahme begründen, dass die elektronische Aufenthaltsüberwachung erforderlich ist, um diese Person durch die Überwachung und die Datenverarbeitung von der Begehung der anlassgebenden Straftaten abzuhalten und Verstöße gegen Aufenthaltsanordnungen oder Kontaktverbote nach § 21 Absatz 2 zu verhüten,
3. das Verhalten dieser Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eine terroristische Straftat begehen wird und die Maßnahme sie von deren Begehung abhalten soll.

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

(2) Die Polizei kann mit Hilfe des von der Person mitgeführten technischen Mittels automatisiert Daten über deren Aufenthaltsort sowie über etwaige Beeinträchtigungen der Datenerhebung verarbeiten. Soweit 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 nach § 19 Absatz 1 Nummer 1, Nummer 2 Buchstabe a, Nummer 2 Buchstabe b und Nummer 2 Buchstabe d oder nach § 21 Absatz 2 Satz 1 oder Absatz 3,
4. zur Verfolgung einer Straftat nach § 106,
5. zur Aufrechterhaltung der Funktionsfähigkeit des technischen Mittels.

Soweit es sich bei den in Satz 7 Nummer 2 in Bezug genommenen Straftaten um Vorfeldstraftaten handelt, kann die Datenverarbeitung nur erfolgen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt. Zur Einhaltung der Zweckbindung nach Satz 7 hat die Verarbeitung der Standortdaten automatisiert zu erfolgen. Die Daten sind gegen unbefugte

Kenntnisnahme und Verarbeitung besonders zu sichern. Die in Satz 1 und Satz 2 genannten Daten sind spätestens zwei Monate nach Beendigung der Maßnahme zu löschen, soweit sie nicht zu Zwecken nach Satz 7 weiterverarbeitet werden. Jeder Abruf der Daten ist gemäß § 32 des Sächsischen Datenschutz-Umsetzungsgesetzes zu protokollieren. Die Protokolldaten sind nach Abschluss der Datenschutzkontrolle nach § 94 zu löschen.

(3) Maßnahmen nach Absatz 1 bedürfen einer richterlichen Anordnung auf 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 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.“

17. 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 Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen.

(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 Rechtsgutgefährdung 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 sowie einzelne gesondert gespeicherte Datensätze aus Internetquellen können ergänzend einbezogen werden, soweit dies zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist. Ein unmittelbarer automatisierter Abgleich mit personenbezogenen Daten im Internet ist unzulässig. 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 Nummer 3 dürfen keine Verkehrsdaten aus Funkzellenabfragen einbezogen werden.

(5) Der Einsatz selbstlernender Systeme ist unter den Voraussetzungen des Absatzes 2 Nummer 1 zulässig, im Übrigen jedoch nur, wenn

1. 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
2. die Maßnahme zur Verhütung dieser Straftat erforderlich ist.

(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, da 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.

Im Rahmen von Maßnahmen nach Absatz 2 ist die Erstellung eines Verhaltensprofils nach Absatz 6 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, Absatz 3 Satz 1 und 2 sowie Absatz 4 entsprechend.

(9) Der Zugang zu einem automatisierten System, mit dem Maßnahmen nach § 62a Absatz 2 und 5 umgesetzt werden, ist auf bestimmte qualifizierte Polizeibedienstete zu beschränken und es ist eine Zugriffskontrolle sicherzustellen. Für die Protokollierung von Maßnahmen nach den Absätzen 2 und 5 gilt § 75 Absatz 1 mit der Maßgabe, dass auch das eingesetzte automatisierte System 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.

(10) Das Staatsministerium des Innern hat das Nähere zum Verfahren zu Maßnahmen nach den Absätzen 2 und 5 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,

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

§ 62b

Anlassbezogene nachträgliche Fernidentifizierung

(1) Die Polizei kann zur Abwehr von Gefahren 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 Gewinnung anderer Informationen über eine Person erforderlich ist. Der Abgleich muss zur Abwehr von Gefahren 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, oder
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 Straftat um eine Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen.

(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. § 79a findet keine Anwendung. 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 spurlos 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.“

18. § 63 Absatz 2 wird durch folgenden § 63 Absatz 2 ersetzt:

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

1. die für eine Gefahr nach den §§ 6 oder 7 Verantwortlichen oder unter den Voraussetzungen des § 9 über Personen, die für die Gefahr nicht verantwortlich sind, wenn dies erforderlich ist zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leben, Gesundheit oder Freiheit einer Person oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, erforderlich ist,
2. Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie in absehbarer Zeit eine zumindest ihrer Art nach konkretisierte Straftat von erheblicher Bedeutung begehen werden,
3. Personen, bei denen das Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eine terroristische Straftat begehen werden, oder
4. Kontakt- und Begleitpersonen der Personen nach den Nummern 2 und 3.

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

19. § 64 wird durch folgenden § 64 ersetzt:

„§ 64

Einsatz einer V-Person, Verdeckte Ermittlerin und Verdeckter Ermittler

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

1. von Polizeibediensteten, die unter einer ihnen verliehenen, auf Dauer angelegten, veränderten Identität (Legende) ermitteln (Verdeckte Ermittlerin, Verdeckter Ermittler), oder
2. einer Person, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist (V-Person).

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

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

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

(5) Als V-Person darf nicht 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.“

20. 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.
21. Die §§ 66 bis 68 werden durch die folgenden §§ 66 bis 68 ersetzt:

„§ 66

Überwachung der Telekommunikation

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

1. die nach den §§ 6 oder 7 verantwortlich ist und wenn die Maßnahme erforderlich ist zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leib, Leben oder Freiheit einer Person oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt,
2. bei der Tatsachen die Annahme rechtfertigen, dass sie in absehbarer Zeit eine zumindest ihrer Art nach konkretisierte Straftat gemäß § 100a Absatz 2 der Strafprozessordnung, die sich gegen die Rechtsgüter nach Nummer 1 richtet, begehen wird und im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für ein solches Rechtsgut vorliegen,
3. deren Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eine terroristische Straftat begehen wird,
4. bei der Tatsachen die Annahme rechtfertigen, dass eine Person nach den Nummern 1 bis 3 deren Telekommunikationsanschluss oder Endgerät benutzt, oder
5. bei der Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach den Nummern 1 bis 3 bestimmte Mitteilungen entgegennimmt oder von dieser herrührende Mitteilungen weitergibt.

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

(2) Die Überwachung und Aufzeichnung der Telekommunikation kann unter den Voraussetzungen des Absatzes 2a auch in der Weise erfolgen, dass mit technischen

Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und
2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unveränderter Form zu ermöglichen.

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

1. die nach den §§ 6 oder 7 verantwortlich ist und wenn die Maßnahme erforderlich ist zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Existenz der Menschen berührt,
2. bei der Tatsachen die Annahme rechtfertigen, dass sie in absehbarer Zeit eine zumindest ihrer Art nach konkretisierte Straftat gemäß § 100a Absatz 2 der Strafprozessordnung, die sich gegen die Rechtsgüter nach Nummer 1 richtet, begehen wird und im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für ein solches Rechtsgut vorliegen,
3. deren Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eine terroristische Straftat begehen wird,
4. bei der Tatsachen die Annahme rechtfertigen, dass 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 3 in Bezug genommenen Straftat um eine Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen. Die Datenerhebung ist nur zulässig, wenn die Abwehr der Gefahr oder die Verhütung der Straftat auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

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

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

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

(4) Maßnahmen nach 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.

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

(6) Maßnahmen nach Absatz 2, die praktische Anwendung und die Auswirkungen dieser Vorschrift werden nach einem Erfahrungszeitraum von drei Jahren, spätestens jedoch zum 31. Dezember 2029 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 1 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 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 Kartennummer von zur Telekommunikation nutzbaren Endgeräten oder
2. des Standortes eines zur Telekommunikation nutzbaren Endgerätes

gilt § 66 Absatz 1 entsprechend.

(2) Die Polizei kann, soweit dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer vermissten, hilflosen oder suizidgefährdeten Person oder einer gefährdeten Person, die einen Notruf über eine öffentlich bekannt gegebene Telefonnummer der Polizei ausgelöst hat, den Standort eines ihr zuzuordnenden mobilen Endgerätes ermitteln, wenn die Ermittlung des Aufenthaltsortes auf andere Weise weniger Erfolg versprechend oder erschwert wäre. Unter den Voraussetzungen des Satzes 1 kann die Polizei von jedem Diensteanbieter 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.“

22. § 69 wird gestrichen.

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

„§ 70

Erhebung von Bestandsdaten

(1) Die Polizei kann von einem Diensteanbieter oder einem Anbieter nach § 2 Absatz 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 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.“

24. § 72 wird gestrichen.

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

„§ 73

Anordnung, gerichtliche Zuständigkeit

(1) Für gerichtliche Entscheidungen nach diesem Gesetz gelten die folgenden Absätze, 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 vorliegen. 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 2 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 5 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 2 die Beteiligten der betroffenen Telekommunikation,
13. bei Erhebung von Nutzungsdaten nach § 67 Absatz 1 Satz 2 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.“

26. In § 76 Absatz 2 Satz 3 wird die Angabe „§ 61 Absatz 3“ durch die Angabe „§ 61 Absatz 2“ ersetzt.
27. § 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.
28. 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 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 erlangt wurden, gilt Absatz 2 Nummer 2 Buchstabe b mit der Maßgabe, dass im Einzelfall eine Gefahrenlage im Sinne des § 65 Absatz 1 Satz 1 oder Absatz 2 Satz 2 vorliegen muss. Personenbezogene Daten, die

durch Herstellung von Lichtbildern oder Bildaufzeichnungen über eine Person im Wege eines verdeckten Einsatzes technischer Mittel in oder aus Wohnungen erlangt wurden, dürfen nicht zu Strafverfolgungszwecken weiterverarbeitet werden. Für die Weiterverarbeitung erlangter personenbezogener Daten, die durch einen Eingriff in informationstechnische Systeme durch die Polizei eines anderen Landes oder des Bundes erhoben wurden, muss im Einzelfall eine Gefahrenlage im Sinne des § 49 Absatz 1 des Bundeskriminalamtgesetzes vorliegen.

(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 von Absatz 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 zur zeitlich befristeten Dokumentation polizeilichen Handelns gespeichert sind, nach Maßgabe des § 79a Absatz 2 weiterverarbeiten. Für die Weiterverarbeitung von Protokolldaten gilt § 32 Absatz 1 des Sächsischen Datenschutz-Umsetzungsgesetzes.

§ 79c

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

(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 Dritte oder Auftragsverarbeiter übermitteln, soweit dies für die Aufgabenerfüllung und für die Entwicklung, das Training oder das Testen des jeweiligen IT-Systems erforderlich ist. Soweit personenbezogene Daten zu Trainingszwecken 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. 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 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. Können diese Zwecke mit pseudonymisierten Daten nicht erreicht werden oder ist die Pseudonymisierung nur mit unverhältnismäßigem Aufwand möglich, dürfen personenbezogene Daten zum Zweck der Entwicklung des Trainings oder des Testens verarbeitet werden. 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 oder die Deanonymisierung von Daten nach Satz 1 ist unzulässig.

(3) Personenbezogene Daten dürfen zur Entwicklung, zum Testen und Trainieren von IT-Systemen nur an Auftragsverarbeiter übermittelt werden, wenn eine Verarbeitung bei der Polizei selber nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. An Dritte dürfen die Daten nur übermittelt werden, wenn eine Verarbeitung durch die Polizei auch unter Zuhilfenahme eines Auftragsverarbeiters 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) Auftrags- und Drittverarbeiter 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 weitenutzen, wenn die Polizei dem 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 das Staatsministerium des Innern in einer nach Anhörung der oder des Sächsischen Datenschutz- und Transparenzbeauftragten zu erlassenden Verwaltungsvorschrift technisch-organisatorische 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 sowie
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 Zeugen in Betracht kommen,
2. sie als Opfer einer künftigen Straftat in Betracht kommen,
3. es sich um Hinweisgeberinnen und -geber und sonstige Auskunftspersonen handelt oder
4. es sich um Kontakt- und Begleitpersonen der Personen nach § 80 Absatz 1 Nummer 1 bis 3 handelt.

Die vorsorgende Speicherung zu Personen nach Satz 1 Nummer 1 bis 3 darf ohne Einwilligung der Person nur dann erfolgen, wenn das Bekanntwerden der Speichungsabsicht 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 einer Person nach den §§ 80 bis 80b erforderlich ist. Die Speicherung der Daten sonstiger Personen darf nicht recherchefähig erfolgen. Zu sonstigen Personen dürfen vorsorgend gespeichert werden nur der Name, das Geburtsdatum, Adressdaten und Daten zur Erreichbarkeit sowie die Angabe, in Bezug auf welche Eigenschaft der Person im Sinne von Satz 1 und in Bezug auf welchen Sachverhalt deren Speicherung erfolgt. Für die weitere Verarbeitung der Daten nach Satz 1 gilt § 79a Absatz 2.

§ 80d

Dauer der Speicherung, Aussonderungsprüffristen, Höchstspeicherfristen

(1) Personenbezogene Daten dürfen solange gespeichert werden, wie dies für die Erfüllung der konkreten Aufgabe und des Zwecks, zu dem sie erhoben worden sind, erforderlich ist. Die Dauer der Speicherung ist auf das erforderliche Maß zu beschränken. Hierzu sind Fristen festzulegen, zu denen spätestens zu prüfen ist, ob die Speicherung für die Erfüllung der Aufgaben noch erforderlich ist (Aussonderungsprüffristen). Die Aussonderungsprüffristen dürfen bei Erwachsenen fünf Jahre, bei Jugendlichen drei Jahre und bei Kindern zwei Jahre nicht überschreiten und beginnen an dem Tag, an dem die Polizei Kenntnis von dem Ereignis erlangt hat. 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 dem siebten Lebensjahr zwei Jahre,
 - b) in Bezug auf sonstige Straftaten bei Erwachsenen drei Jahre, bei Jugendlichen zwei Jahre und bei Kindern ab dem siebten Lebensjahr 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 dem siebten Lebensjahr 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 hinzugegetreten, kann eine erneute Aussonderungsprüffrist nach Absatz 3 Satz 1 bestimmt werden; anderenfalls sind die Daten zu löschen. In den Fällen des

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

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

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

1. von der vorsorgenden Speicherung ausgenommene Sachverhalte,
2. Anforderungen an die erforderliche Prüfung, die Zulässigkeit und den Umfang der vorsorgenden Speicherungen nach den §§ 80 bis 80c,
3. Anforderungen an die erstmalige Festsetzung, die Verlängerung und an Ausnahmen von der Verlängerung von Aussonderungsprüffristen nach den Absätzen 2 bis 4,
4. bestehende 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 Dokumentationspflichtengewährleistet.“

29. § 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.

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

„§ 83

Übermittlungsverbote und Verweigerungsgründe

Übermittlungen nach den Vorschriften dieses Gesetzes haben zu unterbleiben,

1. wenn für die übermittelnde Stelle erkennbar ist, dass unter Berücksichtigung der Art der Daten und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Person das Allgemeininteresse an der Übermittlung überwiegen, oder
2. besondere Verwendungsregelungen entgegenstehen; die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

Die Datenübermittlung unterbleibt darüber hinaus,

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

wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung der Daten zu den in der Charta der Grundrechte der Europäischen Union enthaltenen Grundsätzen, insbesondere dadurch, dass durch die Nutzung der übermittelten Daten im Empfängerstaat Verletzungen von elementaren rechtsstaatlichen Grundsätzen oder Menschenrechtsverletzungen drohen, in Widerspruch steht; die verantwortliche Polizeidienststelle hat die Entscheidung auf der Grundlage der vom Bundeskriminalamt gemäß § 28 Absatz 3 des Bundeskriminalamtgesetzes zu führenden Aufstellung über die Einhaltung der elementaren rechtsstaatlichen Grundsätze und Menschenrechtsstandards sowie das Datenschutzniveau in Drittstaaten zu treffen.

§ 84

Datenübermittlung im innerstaatlichen Bereich

(1) Die Polizei kann unter Beachtung des § 79a Absatz 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.“

31. § 86 wird durch folgenden § 86 ersetzt:

„§ 86

Aufzeichnung von Notrufen und Anrufen, Erhebung von Standortdaten

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

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

(3) Aufzeichnungen und dazugehörige gespeicherte Daten nach Absatz 1 oder 2 sind spätestens nach 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.“

32. § 88 wird durch den folgenden § 88 ersetzt:

„§ 88

Zuverlässigkeitsüberprüfung zum Schutz von besonders gefährdeten Veranstaltungen

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

(2) Die Zuverlässigkeitsüberprüfung darf nur durchgeführt werden, wenn:

1. die betroffene Person zugestimmt hat,
2. dies insbesondere im Hinblick auf den Zugang der betroffenen Person zu einer besonders gefährdeten Veranstaltung und das berechtigte Interesse des Veranstalters erforderlich ist und
3. dies im Hinblick auf den Anlass der Überprüfung, insbesondere den Zugang der betroffenen Person zu der Veranstaltung, mit Rücksicht auf ein berechtigtes Sicherheitsinteresse des Empfängers angemessen ist.

Vor der Zustimmung ist die betroffene Person zu informieren über

1. den konkreten Ablauf der Zuverlässigkeitsüberprüfung
2. den Inhalt der Übermittlung an die in Absatz 4 genannten Stellen,
3. die mit der Überprüfung verbundenen Datenverarbeitungen,
4. die Erkenntnisse, die zur Bewertung, dass Bedenken gegen die Zuverlässigkeit bestehen, führen können und
5. die Möglichkeit der Verweigerung oder des jederzeitigen Widerrufs der Zustimmung.

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

1. der Polizeien von Bund und Ländern,
2. der Strafverfolgungsbehörden und Gerichte, soweit Erkenntnisse über Strafverfahren vorliegen,
3. des Bundesamtes für Migration und Flüchtlinge,
4. des Landesamtes für Verfassungsschutz, soweit im Einzelfall erforderlich sowie
5. der zuständigen Polizeien im Ausland, sofern die zu überprüfende Person ihren Wohnsitz im Ausland hat und dies im Einzelfall erforderlich ist.

(4) Die Polizei darf zum Zweck des Datenabgleichs die erforderlichen personenbezogenen Daten der betroffenen Person an die in Absatz 3 Satz 2 genannten Stellen übermitteln. Personenbezogene Daten, die die Polizei bei diesen Stellen zum Zweck der Durchführung der Zuverlässigkeitsüberprüfung erhoben hat, 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 Vorliegen von Zuverlässigkeitsbedenken. Die betroffene Person ist über den Inhalt der Übermittlung zu informieren.

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

(6) Die Polizei kann die im Rahmen der Zuverlässigkeitsüberprüfung verarbeiteten personenbezogenen Daten 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.“

33. Nach § 89 wird folgender § 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 Informationersuchen 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.“

34. § 91 wird durch folgenden § 91 ersetzt:

Berichtigung, Löschung und Einschränkung der Verarbeitung

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

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

1. ihre Speicherung unzulässig war,
2. sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen,
3. die weitere Speicherung unzulässig ist, weil die Ermittlungen oder eine der Polizei bekannte Entscheidung der Staatsanwaltschaft oder eines Gerichts ergeben, dass die Gründe, die zu der Speicherung geführt haben, nicht zutreffen,
4. aus Anlass einer Einzelfallbearbeitung oder aus Anlass des Ablaufs einer Aussonderungsprüffrist festgestellt wird, dass ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist,
5. nach Ablauf der Aussonderungsprüffrist die Umstände, die zur Speicherung geführt haben, entfallen sind,
6. die Höchstspeicherfrist abgelaufen ist,
7. die betroffene Person die Einwilligung für die Speicherung widerrufen hat, oder
8. zwei Jahre nach dem Tod der betroffenen Person vergangen sind.

(3) Sind personenbezogene Daten in Akten gespeichert und wird deren Unrichtigkeit festgestellt, ist die Berichtigungspflicht nach § 31 Absatz 1 des Sächsischen Datenschutz-Umsetzungsgesetzes dadurch zu erfüllen, dass dies in der Akte vermerkt wird. Bestreitet die betroffene Person die Richtigkeit sie betreffender personenbezogener Daten und lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, sind die Daten zu kennzeichnen, um eine Einschränkung der Verarbeitung gemäß § 14 Absatz 1 Satz 3 des Sächsischen Datenschutz-Umsetzungsgesetzes zu ermöglichen. Die Verarbeitung personenbezogener Daten in Akten ist einzuschränken, wenn Daten

1. nach Absatz 2,
2. auf Grund von sonstigen durch dieses Gesetz bestimmten Löschungsverpflichtungen oder
3. nach § 14 Absatz 2 des Sächsischen Datenschutz-Umsetzungsgesetzes

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

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

35. In § 93 Absatz 1 Nummer 10 wird die Angabe „personellen,“ gestrichen und die Angabe „27“ durch die Angabe „20“ ersetzt.
36. § 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 5 und 6, § 62b Absatz 2 sowie den §§ 63 bis 68, auch im Hinblick auf die Datenverarbeitung in polizeilichen Dateisystemen, und“.
37. In § 97 Absatz 1 Nummer 3 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.
38. In § 101 Absatz 1 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.
39. § 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.“
40. Nach § 106 wird folgender § 106a eingefügt:

„§ 106a

Ordnungswidrigkeiten

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

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

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

41. § 107 wird durch folgenden § 107 ersetzt:

„§ 107

Berichtspflichten gegenüber dem Landtag

Das Staatsministerium des Innern berichtet der Öffentlichkeit und dem Landtag jährlich über abgeschlossene Maßnahmen nach § 21 Absatz 2 und 3, § 57 Absatz 4 Satz 2 und Absatz 5 Satz 2, § 57a Absatz 1 Satz 4 und Absatz 2, § 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.“

42. § 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. § 40 wird wie folgt geändert:
 - a) In Absatz 4 Satz 2 wird nach der Angabe „Als Waffen“ die Angabe „von Spezialeinheiten“ eingefügt.
 - b) Absatz 5 wird gestrichen.
2. § 57 wird wie folgt geändert:
 - a) Absatz 4 wird wie folgt geändert:
 - aa) Die Sätze 2 und 3 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) In Absatz 8 werden die Sätze 6 und 7 gestrichen.
 - d) Absatz 10 wird gestrichen.
3. § 62a Absatz 4 Satz 5 Nummer 2 wird durch folgende Nummer 2 ersetzt:

„2. personenbezogene Daten, die aus einer Wohnraumüberwachung gewonnen wurden oder von nach § 79a Absatz 4 Satz 3 erlangten Daten, und“
4. § 66 wird wie folgt geändert:
 - a) Die Absätze 2 und 3 werden gestrichen.
 - b) Absatz 4 wird zu Absatz 2 und die Angabe „den Absätzen 1 und 2“ durch die Angabe „Absatz 1“ ersetzt.
 - c) Absatz 6 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 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 folgenden Absatz 1 ersetzt:

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

1. an, in oder in unmittelbarer Nähe von öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Kulturgütern, Dienstgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen künftig Straftaten oder Ordnungswidrigkeiten begangen werden, durch die Personen oder Sach- oder Vermögenswerte gefährdet werden, oder
2. in öffentlich zugänglichen Bereichen sonstige erhebliche Gefahren für die öffentliche Sicherheit entstehen,

und die Bildaufnahmen und -aufzeichnungen zur Abwehr dieser Gefahren erforderlich sind.“

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

„(1) Soweit die Polizeibehörden personenbezogene Daten zur Erfüllung ihrer Aufgaben verarbeiten, die in den Anwendungsbereich von § 1 des Sächsischen Datenschutz-Umsetzungsgesetzes fallen, gelten die §§ 54 bis 56, § 79 Absatz 1 und 2, § 79a 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 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 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 Absatz 1, 2, 3 Satz 1 und 2 sowie Absatz 4 wird jeweils die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

Artikel 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

(1) Dieses Gesetz tritt vorbehaltlich der Absätze 2 bis 4 am Tag nach der Verkündung in Kraft.

(2) Artikel 1 Nummer 11 tritt am 1. Januar 2027 in Kraft.

(3) Artikel 2 Nummer 2 bis 4 tritt am 31. Dezember 2031 in Kraft.

(4) Artikel 2 Nummer 1 tritt am 31. Dezember 2032 in Kraft.

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)

Begründung

A. Allgemeiner Teil

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

I. Änderungsbedarf in Folge von höchstrichterlicher Rechtsprechung

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

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

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

Ferner sind umzusetzen:

- die Anpassung der Nachtzeitregelung von 4 auf 6 Uhr im Rahmen der Durchsuchung von Wohnungen (BVerfG Beschluss 12.03.2019, 2 BvR 675/14) und
- die Stärkung des Kernbereichsschutzes auf der Erhebungs-, Auswertungs- und Verwertungsebene beim Einsatz von verdeckten Ermittlerinnen, verdeckten Ermittlern und V-Personen (BVerfG Beschluss vom 09.12.2022, 1 BvR 1345/21).

II. Regelungsbedarfe in Umsetzung des Koalitionsvertrages

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

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

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

1. Umsetzung von EU-Recht

Die 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 trifft Vorgaben zum Informationsaustausch mit EU-Mitgliedstaaten und Schengen-assoziierten Staaten zum Zweck der Verhütung, Aufdeckung oder Untersuchung von Straftaten. Ziel der bis zum 12. Dezember 2024 mitgliedstaatlich umzusetzenden Richtlinie ist eine Verbesserung des bestehenden Rechtsrahmens zum Informationsaustausch, um insbesondere auf grenzüberschreitende kriminelle Aktivitäten reagieren zu können. Aufgrund unterbliebener Notifizierung der Umsetzung hat die Europäische Kommission ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet. Auf Bundesebene wurden zwischenzeitlich ein Gesetzgebungsverfahren zur Umsetzung der Richtlinie im Bundeskriminalamtgesetzes, im Bundespolizeigesetz und in weiteren Vorschriften initiiert. Vor dem Hintergrund dieser Gesetzesinitiativen und von Abstimmungen zwischen Bund und Ländern, wird nunmehr in § 89a eine Regelung zur Umsetzung dieser Richtlinie in das Sächsische Polizeivollzugsdienstgesetz im Kontext der Vorschriften über die grenzüberschreitende Datenübermittlung aufgenommen.

Ein wesentliches Ziel der Novellierung ist die Verbesserung des Schutzes von Opfern und potenziellen Opfern häuslicher Gewalt. Durch das Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (Istanbul-Konvention), das am 1. Februar 2018 in Deutschland in Kraft trat, ist die Bundesrepublik auf sämtlichen Verwaltungsebenen dazu verpflichtet, Gewalt gegen Frauen und häusliche Gewalt zu verhüten, zu bekämpfen und Betroffenen umfassenden Schutz sowie Unterstützung zu gewähren. In Umsetzung des sächsischen Koalitionsvertrags 2024-2029 ist in den Zif-

fern 3287 bis 3290 festgehalten: "Der Schutz von Frauen vor Gewalt hat für uns einen hohen Stellenwert. Hierzu werden wir die Istanbul-Konvention auf Basis des Landesaktionsplans des Freistaats zur Verhütung und Bekämpfung geschlechtsspezifischer Gewalt umsetzen und die dazu notwendigen Mittel wollen wir verlässlich zur Verfügung stellen.". Das bestehende Instrumentarium zum staatlichen Gewaltschutz umfasst sowohl polizeirechtliche Verfügungen als auch familiengerichtliche Anordnungen nach dem Gesetz zum zivilrechtlichen Schutz vor Gewalttaten und Nachstellungen (Gewaltschutzgesetz). Beide Rechtsregime sehen Schutzmaßnahmen vor, die darauf abzielen, Gewaltausübende fernzuhalten. Dazu gehören Wohnungsverweisungen, Betretungsverbote für Räumlichkeiten, die das Opfer regelmäßig aufsucht sowie Kontakt- und Näherungsverbote. Das vorliegende Gesetz verfolgt das Ziel, die Wirksamkeit dieser Schutzmaßnahmen und deren Durchsetzung gegenüber den bisherigen Regelungen zu erweitern und klarer zu strukturieren und damit den Schutz insgesamt zu verbessern.

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

2. Sonstiger aus polizeifachlicher Sicht bestehender Regelungsbedarf

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

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

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

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

Zum Zweck des Einsatzes von durch die Polizei entwickelter oder genutzter lernender Analysesoftware zur Aufgabenerfüllung wird eine Befugnis aufgenommen, die den gesetzlichen Rahmen für das Training oder den Test von regelbasierten und selbstlernenden Systemen durch die Polizei erlaubt, so beispielsweise zur automatisierten (Verhaltens-)Mustererkennung, (§ 79c-neu).

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

Der Gesetzentwurf sieht weiterhin vor:

- Die Neufassung der Befugnis zur Durchführung von Zuverlässigkeitsüberprüfungen bei besonders gefährdeten Veranstaltungen (§ 88).
- Die Aufnahme von Befugnissen zur Abwehr und zum Einsatz von unbemannten Fahrzeugsystemen in Anpassung an technischen Veränderungen (§§ 12a-neu, 71-neu).
- Die Erweiterung der bestehenden Regelung zur automatisierten Kennzeichenerkennung zur effizienteren Gefahrenabwehr unter Berücksichtigung von Rechtsprechung des Bundesverfassungsgerichts (§ 58).
- Die Aufnahme einer Befugnis zur Standortdatenübermittlung bei Notrufen, um Menschen in Notsituationen metergenau orten zu können (§ 86 Absatz 1-neu).
- Die Aufnahme einer Befugnis zur öffentlichen Ausschreibung von gefährdeten Personen oder von Personen, von denen eine Gefahr ausgeht (§ 84a-neu).
- Die Umbenennung des Polizeiverwaltungsamtes in „Polizeipräsidium für Service und IT“ zur Steigerung der Arbeitgeberattraktivität. Hierzu bedarf es der Folgeanpassung in zahlreichen Gesetzen und Verordnungen (§ 97 und weitere Vorschriften).
- Eine Vielzahl redaktioneller Anpassungen, so u. a. Folgeänderungen in Konsequenz von Änderungen im Bundesrecht und die Behebung sonstiger redaktionelle Versehen.

Artikel 2 trägt dem Umstand Rechnung, dass bestimmte neue Befugnisregelungen nur befristet gelten sollen.

In Artikel 3 sieht der Gesetzentwurf bezüglich des Sächsischen Polizeibehördengesetzes im Wesentlichen die Anpassung an die Rechtsprechung des Sächsischen Verfassungsgerichtshofes zur Zulässigkeit der Videoüberwachung nach § 30 SächsPBG sowie an die Rechtsprechung des BVerfG zur Nachtzeit vor. In Artikel 4 werden die Grundrechte angeführt, in die durch die Artikel 1 und 3 dieses Gesetzes eingegriffen wird.

In Konsequenz der Aufnahme neuer eingriffsintensiver Befugnisse in das Sächsische Polizeivollzugsdienstgesetz erweitert der Gesetzentwurf die Kontrollbefugnisse des Parlamentarischen Kontrollgremiums im Sächsischen Kontrollgesetz (Artikel 5).

Die Änderung durch Artikel 6 dient der gesetzlichen Harmonisierung, die durch die Artikel 7 bis 15 erfolgenden Änderungen betreffen die durch die Umbenennung des bisherigen Polizeiverwaltungsamtes erforderlichen Folgeänderungen. Artikel 16 bestimmt das Inkrafttreten der jeweiligen Artikel.

IV. Gesetzesfolgen

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

1) Haushaltsauswirkungen

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

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

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

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

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

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

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

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

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

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

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

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

Einmalige Kosten fallen infolge einer Evaluierungsverpflichtung zum Einsatz von Bodycams in Wohnungen an (siehe § 57 Absatz 10). Hierzu können – nach den Erfahrungen der letzten Evaluierung zu verschiedenen Vorschriften des Sächsischen Polizeivollzugsdienstgesetzes – Kosten von geschätzt 30.000 bis 50.000 EUR für die Haushaltsjahre 2027 (Abschlagszahlung) und 2028 oder 2029/30 (Restzahlung) angesetzt werden.

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

Im Hinblick auf die neue Befugnis zur „gestuften“ Datenverarbeitung nach § 57a Absatz 1 SächsPVDG wird nach derzeitigem Erkenntnisstand von einem Bedarf von zwei Anlagen pro Polizeidirektion ausgegangen. Zur Realisierung im Jahr 2028 werden Investitionskosten in Höhe von 750.000 EUR geschätzt. Für den jährlichen Sachaufwand werden 200.000 EUR veranschlagt. Aufgrund bestehender Erfahrungen ist davon auszugehen, dass auf der Grundlage bestehender Befugnisregelungen zur Videoüberwachung (§ 57 Absatz 3 SächsPVDG) bereits vorhandene Videoüberwachungstechnik nicht aufrüstungsfähig ist.

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

In der sächsischen Kabinettsvorlage „Digitalisierungspaket Innere Sicherheit“ sind für Themen der Digitalisierungsinfrastruktur 71,3 Mio. EUR (ggf. aus dem Sondervermögen Bund) veranschlagt. Von denen sind auch Mittel für die notwendige Erweiterung bzw. den initialen Aufbau von geeigneten IT-Infrastrukturen eingeplant. Entsprechend sind Umsetzungspotentiale von den tatsächlich zur Verfügung stehenden Mitteln abhängig.

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

Zur Steigerung der Effizienz dieser Maßnahme ist deren verdeckter Einsatz neu vorgesehen (so bereits die Vorgängerfassung § 19a Absatz 1 Satz 4 SächsPolG). Aus polizeifachlicher Sicht besteht Bedarf für den Erwerb von weiteren drei stationären Anlagen. Dabei ist von Investitionskosten in Höhe von insgesamt 150.000 EUR (davon 25.000 EUR für Softwareanpassungen) auszugehen. Für den Betrieb der stationären Anlagen wird für die Jahre 2026 und 2027 ein Betrag in Höhe von insgesamt 350.000 EUR (davon 120.000 EUR für Reparaturen, Updates und Reserve) und für das Jahr 2028 in Höhe von 45.000 EUR angesetzt.

Einmalige Kosten fallen infolge einer Evaluierungsverpflichtung im Hinblick auf die Regelung des stationären Technikeinsatzes an (siehe § 58 Absatz 6). Hierzu können – nach den Erfahrungen der letzten Evaluierung zu verschiedenen Vorschriften des Sächsischen Polizeivollzugsdienstgesetzes – Kosten von geschätzt 30.000 bis 50.000 EUR für die Haushaltsjahre 2027 (Abschlagszahlung) und 2028 oder 2029/30 (Restzahlung) angesetzt werden.

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

Die Erweiterung der Befugnis der elektronischen Aufenthaltsüberwachung auf Hochrisikofälle von häuslicher Gewalt verursacht keine Investitionskosten, jedoch wiederkehrenden Personalaufwand, dessen Umfang fallabhängig ist. Der Umfang der Mehrkosten ist zudem abhängig davon, ob die länderübergreifende Verbundlösung zur Datenverarbeitung (Nutzung der gemeinsamen Überwachungsstelle der Länder mit Sitz in Hessen) durch gesonderte Vereinbarung mit dem Land Hessen fortgesetzt werden kann. Soweit dies möglich ist, entstehen für die Erstanlegung der elektronischen Fußfessel Kosten im mittleren vierstelligen Bereich (5.000 EUR) pro Person, die durch das Land Hessen für die Zurverfügungstellung der Ausstattung mit der „elektronischen Fußfessel“ in Rechnung gestellt werden. Für die Folgemonate können ggf. außergewöhnliche Kosten (Geräte austausch) anfallen, deren Höhe vorab nicht genau beziffert werden können. Es wird von weiteren Sachkosten in Höhe von 25.000 EUR pro Jahr ausgegangen. Nach gegenwärtiger Einschätzung wird von Anwendungsfällen im einstelligen Bereich pro Jahr (ca. fünf Überwachungsfälle wegen häuslicher Gewalt und Stalking) ausgegangen. Stellenmehrbedarf besteht nicht, da die elektronische Aufenthaltsüberwachung andere offene/verdeckte Maßnahmen ergänzen und je nach Einzelsachverhalt Personalressourcen schonen werden, bspw. wenn auf eine personalintensive Observation verzichtet werden kann.

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

- Befugnis zum anlassbezogenen besonderen automatisierten Datenabgleich und zur anlassbezogenen automatisierten Datenanalyse (§ 62a SächsPVDG)

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

Kosten der Personalschulung für die Bedienung der Analysesoftware können aus dem „Digitalisierungspaket Innere Sicherheit“ bestritten werden; für den Bereich Analyse sind in der entsprechenden Kabinettsvorlage 4,025 Mio. EUR eingeplant, die - einen entsprechenden

Mittelfluss vorausgesetzt - auch für entsprechende Schulungsaufwände verwendet werden können. Konkrete Aussagen zur Dauer der Schulung eines Analysten können nicht getroffen werden. Durchschnittlich dauern Schulungen je nach Komplexität einer neuen Software zwischen zwei und vier Tage. Ausgehend von geschätzten drei Schulungstagen und fünf zu schulenden Analysten pro Dienststellen müssten 30 Analysten der LG 2.1 in 720 Stunden ausgebildet werden. Dadurch würden Personalkosten i.H.v. 42.832,80 EURO gemäß Anlage 2 zur VwV SächsNKR entstehen.

- Befugnis zur anlassbezogenen nachträglichen Fernidentifizierung (§ 62b SächsPVDG)

Welche Software zur Umsetzung der neuen Befugnisregelung geeignet ist und in die Auswahl einbezogen wird, kann gegenwärtig nicht eingeschätzt werden. Demzufolge können die voraussichtlichen Kosten für die Beschaffung der Software nicht genau beziffert werden. Die zentrale Beschaffung einer entsprechenden Software für die Polizeien des Bundes und der Länder (vorzugswürdig) erscheint derzeit aufgrund absehbarer Kostensteigerung eher unwahrscheinlich. Für Sachsen wird mit einem Sachaufwand in Höhe von jährlich 60.000 EUR für die Beschaffung der Software im sog. Abo-Modell bei monatlicher Kündigungsmöglichkeit gerechnet. Für die Beschaffung weiterer Lizenzen (Zusatzmodule) ist bei sachsenweit 15 erforderlichen Lizenzen bei einem geschätzten Kostenansatz von 10.000 EUR pro Lizenzgebühr von jährlichen Betriebskosten in Höhe von 150.000 EUR auszugehen. Für die Beschaffung der erforderlichen Monitore werden einmalige Investitionskosten in Höhe von 15.000 EUR veranschlagt. Entsprechende Sachkosten sind in geeigneter Höhe eingeplant und im Polizei-IT-Fond Teil 2 angemeldet.

Fallzahlen für eine solide Aussage zur Anzahl künftiger präventiv durchzuführender Maßnahmen liegen nicht vor, da eine repressive Befugnis in der Strafprozessordnung nicht besteht. Allenfalls kann ein jährliches Fallaufkommen ab 2027 zwischen einem hohen einstelligen Bereich (im ersten Jahr) und einem mittleren zweistelligen Bereich (ca. 50 Fälle) grob geschätzt werden.

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

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

Investitionskosten fallen nicht an, da entsprechende Technik vorhanden ist. Je nach Einzelsachverhalt besteht eine unterschiedliche Anzahl von zu überwachenden Telefonanschlüssen. In der Regel umfasst ein Fall maximal ein bis zwei relevante Anschlüsse, so dass von insgesamt 14 zu überwachenden Anschlüssen pro Jahr schätzungsweise auszugehen ist. Pro Anschluss sind mit Providerkosten als Sachaufwand im unteren vierstelligen Bereich zu rechnen.

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

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

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

- Befugnis zur Entwicklung, Training und Testen von regelbasierten und lernenden IT-Systemen (§ 79c SächsPVDG)

Kosten im Zusammenhang mit der Umsetzung der neuen Befugnis können nicht beziffert werden, da deren Höhe davon abhängig ist, ob entsprechende Software eigenentwickelt wird, externe Dienstleister in Anspruch genommen werden oder einer Bundeslösung (vorzugswürdig) „beigetreten“ werden kann. Welche Software in Betracht kommt, ist derzeit nicht absehbar. Die Ergebnisse und die sich daraus ergebenden Kosten wären nach einer Marktanalyse unter haushälterischen Gesichtspunkten zu begutachten. Neben den Kosten für die zu beschaffende/entwickelnde Software wären zudem nicht bezifferbare Betriebskosten für Server zu berücksichtigen. Für die erforderliche Infrastruktur sind im Sondervermögen des Bundes finanzielle Mittel in Höhe von 71,3 Millionen Euro gemäß Planung vorgesehen (Anteil Sachsens). Grundsätzlich sind diese Mittel dazu geeignet, sofern sie im geplanten Umfang zur Verfügung stehen, das Themenfeld der "lernenden IT-Systeme" abzudecken, einschließlich der nach tatsächlichem Umfang erforderlichen Schulungskosten.

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

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

Der Polizeivollzugsdienst Sachsen nimmt seit dem 8. November 2024 an einem Pilotprojekt zur Implementierung und Pilotierung der Advanced Mobile Location (AML) Technologie teil, das durch Baden-Württemberg federführend für alle Länder betrieben wird. Nach Abschluss der Pilotphase bei der beteiligten Polizeidirektion Dresden ist ein sukzessiver Anschluss aller Polizeidirektionen vorgesehen. Im Rahmen des Pilotprojekts fallen derzeit keine Kosten an. Für den bundesweiten Dauerbetrieb wird jährlich von einem niedrigen sechsstelligen Betrag ausgegangen, der voraussichtlich spätestens ab 2027 über den Königsteiner Schlüssel auf die Länder verteilt wird. Der Anteil Sachsens wird bei ca. 75.000 EUR jährlich liegen. Zusätzliche Kosten für Personal sind nicht zu erwarten.

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

Die mit der Umbenennung verbundenen Sachkosten werden insgesamt mit 20.500 EUR veranschlagt.

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

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

2) Erfüllungsaufwand

a) Erfüllungsaufwand für die Bürgerinnen und Bürger

Das Gesetz bewirkt keinen Erfüllungsaufwand bei Bürgerinnen und Bürgern.

b) Erfüllungsaufwand für die Wirtschaft

Das Gesetz bewirkt keinen Erfüllungsaufwand bei der Wirtschaft

c) Erfüllungsaufwand für die Verwaltung

aa) Polizeivollzugsdienst

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

Demzufolge ist der dem Polizeivollzugsdienst entstehende einmalige sowie wiederkehrende Mehraufwand infolge der Neuregelungen sowohl hinsichtlich des Umfangs, als auch im Hinblick auf die zeitliche Einordnung grundsätzlich nicht ermittelbar bzw. kann allenfalls nur grob geschätzt werden. Dabei kann grundsätzlich davon ausgegangen werden, dass infolge von Technikeinsatz, insbesondere durch neue Softwarelösungen, die Polizeiarbeit insgesamt erleichtert wird, wodurch einerseits Zeitersparnisse entstehen und andererseits Personalressourcen eingespart werden bzw. in der Gesamtbilanz nicht zu einem höheren Aufwand in der Gesamtbewältigung eines Gefahrensachverhaltes führen. Jedoch können vollständige Aussagen zum Personalaufwand im Zusammenhang mit technischen Befugnissen, insbesondere zum § 79c SächsPVDG, nicht mit seriösen Zahlen oder zuverlässigen Schätzungen getroffen werden.

Die seit 2026 erfolgte flächendeckende Einführung der elektronischen Akte sowohl bei den Dienststellen der Sächsischen Polizei im System VIS-Polizei als auch bei der sächsischen Justiz im System VIS-Justiz wird keine Auswirkungen auf den Erfüllungsaufwand zum vorliegenden Gesetzentwurf haben, weil derzeit beide Systeme nur für Strafverfolgungszwecke technisch eingerichtet wurden und betrieben werden dürfen.

Im Einzelnen kann der Erfüllungsaufwand zum Personaleinsatz wie folgt angegeben werden:

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

Es wird von 15 bis 20 überwiegend mehrtägigen Einsatzlagen pro Jahr ausgegangen. Für die reine Einsatzzeit fallen bei 20 Einsätzen pro Jahr insgesamt ca. 200 Stunden für den Polizeivollzugsdienst (PVD) der Laufbahngruppe (LG) 2.1 und ca. 1.600 Stunden der LG 1.2 im Jahr an. Dies entspricht ca. 88.506 EUR pro Jahr (vgl. Lohnkostentabelle IV. der Anlage 2 zur VwV SächsNKR) Personalkosten für Einsätze.

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

Personalkosten entstehen in Form von Schulungsmaßnahmen für den Tasereinsatz. Die Schulungen sollen 16 Stunden pro Einsatzbeamten umfassen. Als erster Richtwert für die Anzahl der auszubildenden Beamten wird von 540 PVD der LG 1.2 und 2.1 ausgegangen. Das entspricht Personalkosten in Höhe von ca. 463.838 EUR bei hälftiger Teilnahme beider Laufbahngruppen. Hinzu treten Personalkosten für zwei Polizeitrainer in jeweiliger Höhe eines Jahresgehalts.

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

Personalkosten für die Durchführung von Analysen können nur grob geschätzt werden und sind abhängig vom jeweiligen Ausgangssachverhalt und vom Umfang des Fallaufkommens pro Jahr in jeder Polizeidienststelle. Umfangreiche Analysen können mehrere Stunden pro Arbeitstag andauern und im Falle einer stationären Videoüberwachung gemäß § 57 Abs. 3 SächsPVDG können mehrere Arbeitstage über einen Zeitraum von drei bis sechs Monaten erforderlich sein; hingegen Analysen zur Videoüberwachung auf Grundlage des § 57 Abs. 2 SächsPVDG auch nur wenige Stunden andauern können. Seriöse Aussagen sind, auch zu Durchschnittswerten, daher nicht möglich. Die Anzahl der Fälle pro Jahr kann aufgrund fehlender Erfahrungswerte allenfalls grob geschätzt werden; ab dem Jahr 2028 ist anfangs von einem anwachsenden Fallaufkommen im mittleren einstelligen Bereich pro Jahr auszugehen

Weitere Personalkosten entstehen aufgrund der Prüfungspflicht gemäß Abs. 4 Satz 4 in Höhe von ca. 59,49 EUR (ca. eine Stunde für einen PVD der LG 2.1) pro Anwendungsfall eines Abgleichs, aufgrund der schriftlichen Antragstellung für die richterliche Genehmigung gemäß Absatz 5 Satz 2 in Höhe von 118,98 EUR (ca. zwei Stunden pro Anwendungsfall für einen PVD der LG 2.1) sowie in Höhe von 30 Minuten (29,75 EUR) für die nach Absatz 6 Satz 4 geregelte Unterrichtungspflicht gegenüber der Sächsischen Datenschutz- und Transparenzbeauftragten.

Größerer Erfüllungsaufwand entsteht für die nach Abs. 6 Satz 7 geregelten Mitteilungspflichten nach Art. 5 Absatz 4 KI-VO [Verordnung (EU) 2024/1689] sowie Betreiberpflichten bei der Verwendung von Hochrisiko-KI-Systemen gemäß den Vorgaben des Art. 26 KI-VO.

Nach Art. 5 Absatz 4 ist für jede Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems eine Mitteilung nach den Vorgaben des Absatz 6 zu erstellen und an die zuständigen Marktüberwachungsbehörden und Datenschutzbehörden zu senden. Die Anzahl der Fälle pro Jahr kann aufgrund fehlender Erfahrungswerte allenfalls grob mit maximal drei Analysen geschätzt werden, wobei für eine Mitteilung von einem Arbeitsaufwand für einen Bediensteten der Laufbahngruppe (LG) 2.1 in Höhe von ca. einer Stunde auszugehen ist.

Nach Art. 26 Absatz 10 ist ein Jahresbericht über die Verwendung der genutzten (Analyse)Systemen zu erstellen und den zuständigen Marktüberwachungsbehörden und Datenschutzbehörden vorzulegen. Für die Erstellung eines Jahresberichts ist mit einem Personalaufwand in Höhe von geschätzten 24 Arbeitsstunden für einen Bediensteten der Laufbahngruppe (LG) 2.1 zu rechnen. Dies entspricht ca. 1.427,76 EUR pro Jahr (vgl. Lohnkostentabelle IV. der Anlage 2 zur VwV SächsNKR) Personalkosten.

Kosten der Personalschulung für die Bedienung der Analysesoftware entstehen nur für Neu-/Erstanwender im Umfang von ca. 4 Arbeitsstunden pro PVD (237,96 EUR). Weitere Personalkosten entstehen im Umfang von sog. Zentralstellenaufgaben wie Wartung und Support; hierzu wird von einem Personaleinsatz von zwei PVD pro Dienststelle und fünf PVD im PVA bzw. im LKA ausgegangen, wobei die Anzahl der erforderlichen Arbeitsstunden für die PVD pro Jahr nicht bezifferbar ist.

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

Zusätzliche Personalkosten fallen keine an, weil durch den Einsatz stationärer Anlagen die Einsatzzeit für mobile, personalintensiven Anlagen entsprechend reduziert wird. Eine seriöse Aussage über den Umfang der Arbeitszeitreduzierung kann nicht getroffen werden, da derzeit nicht zuverlässig prognostizierbar ist, in welchem Umfang die mobilen Anlagen neben den zukünftig vier stationären Anlagen genutzt werden. Mobile Anlagen erfordern einen Vor-Ort-Einsatz von zwei Beamten der LG 1.2, hingegen Treffermeldungen bei stationären Anlagen im Führungs- und Lagezentrum auflaufen und zusammen mit anderen eingehenden Meldungen im täglichen Dienst abgearbeitet werden. In 2024 erfolgten zu 27 stationären Kontrollmaßnahmen 113 Einsatzstunden und 454 Treffermeldungen und zu 37 mobilen Kontrollmaßnahmen 144 Einsatzstunden und 215 Meldungen.

Ausgehend von einer durchschnittlichen Einsatzdauer von vier Stunden zzgl. einer weiteren geschätzten Stunde für An- und Abfahrt inkl. Auf- und Abbau der Anlage entstehen für den PVD beim Betrieb einer mobilen Anlage Personalkosten in Höhe von 478,80 EUR (gemäß Anlage 2 zur VwV SächsNKR) pro Einsatz. Während der Einsatzzeit erfolgt die Trefferauswertung. Beim Betrieb einer stationären Anlage entfallen Kosten für die An- und Abfahrt inkl. Auf- und Abbau der Anlage (Arbeitszeit). Personalkosten für einen Beamten der LG 2.1 entstehen lediglich für die Trefferauswertung während einer durchschnittlichen vierstündigen Inbetriebnahme der Anlage. Im Jahr 2024 erfolgten während dieser Zeit durchschnittlich 16 Treffermeldungen, davon 1,3 Echttreffer (8,2%). Die Auswertung einer Treffermeldung dauert ca. eine Minute bei sog. Systemtreffern und die Auswertung von Echttreffern erfordert eine Datenprüfung von weniger als fünf Minuten, so dass von einer geschätzten Arbeitszeit in Höhe von 20 Minuten (19,83 EUR) auszugehen ist. Die Ersparnis an Personalkosten bei einem stationären Einsatz gegenüber den Kosten bei einem mobilen Einsatz liegt bei 458,97 EUR pro vierstündigem Einsatz.

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

Mit der Erweiterung der Ausschreibung auf die Ermittlungsanfrage ist im Anwendungsfall ein Zeit- und Arbeitsaufwand verbunden, der in der Höhe vom bundesweiten Anfrageaufkommen an sächsische Dienststellen abhängig ist. Die Anfrage führt in der Gesamtbilanz nicht zu einem höheren Aufwand in der Gesamtbewältigung des Gefährdungssachverhalts, weil sich lediglich die polizeiliche Bearbeitungsweise ändern wird: anstelle einer Anfrage per individuellem Fernschreiben oder E-Mail wird zukünftig eine bundesweite Ausschreibung zur Ermittlungsanfrage erfolgen. Es ist nicht davon auszugehen, dass sich der Informationsbedarf durch die Einführung der Ermittlungsanfrage gegenüber dem Status Quo bundesweit signifikant erhöhen wird. Seriöse Aussagen über die Anzahl der Ermittlungsanfragen in den sechs Dienststellen pro Jahr können nicht getroffen werden. Ein Vergleich zum Gesetzesvorhaben des Bundes zeigt, dass die Bundespolizei von 150 Anfragen zu jeweils drei Arbeitsstunden pro Jahr für PVD der LG 2.1 ausgeht. Davon ausgehend wäre in Sachsen schätzungsweise mit 50 Anfragen zu rechnen, wobei die Anzahl an Ausschreibungen über die Jahre mit zunehmender Akzeptanz ansteigen wird. Hochgerechnet mit drei Arbeitsstunden eines Beamten der LG 2.1 pro Ausschreibung entstehen Personalkosten i.H.v. 8.923,50 EURO (gemäß Anlage 2 zur VwV SächsNKR).

- Befugnis zum anlassbezogenen besonderen automatisierten Datenabgleich und zur anlassbezogenen automatisierten Datenanalyse (§ 62a SächsPVDG)

Mit Einführung und Umsetzung der Maßnahme werden gegenüber einer bisherigen händischen Analyse erhebliche Personalressourcen eingespart:

- Die Durchführung einer automatisierten Analyse reduziert erheblich die Arbeitszeit des Analysten, der bislang mehrere manuelle Arbeitsschritte durchführen muss, wie bspw. die Datenaufbereitung, mehrfache manuelle Erfassung der Suchkriterien für die Recherche in verschiedenen Datensystemen und Dateien, Qualitätssicherungen für Trefferanzeigen, manuelle Stichprobenkontrollen für Redundanzen sowie Fertigung von Kontrollübersichten

und ggf. Zwischenergebnissen. Erfahrungen aus anderen Ländern zur Effizienz der automatischen Datenanalyse zeigen, dass durch den Einsatz der Software eine wochenlange Auswertung vermieden werden konnte. Angaben zur Anzahl der Fälle pro Jahr können allenfalls anhand von Vergleichszahlen aus anderen Ländern geschätzt werden. Die bayerische Polizei veröffentlichte für einen Zeitraum von neun Monaten mehr als 80 Anwendungsfälle, so dass für Sachsen ab 2028 von einem niedrigen dreistelligen Fallaufkommen auszugehen ist (grobe Schätzung), wobei die Anzahl über die Jahre mit zunehmender Akzeptanz ansteigen wird. Ausgehend von 100 Maßnahmen pro Jahr ergibt das einen Personalaufwand für die genannten Pflichten i.H.v. 23.796 EURO gemäß Anlage 2 zur VwV SächsNKR. Analysten gehören in der Regel der LG 2.1 an.

- Weitere Personalkosten entstehen aufgrund der Prüfungs- und Dokumentationspflicht gemäß Abs. 7 Satz 2, 3 und 5 in Höhe von ca. 59,49 EUR (ca. eine Stunde für einen PVD der LG 2.1) pro Anwendungsfall einer Analyse, aufgrund der Begründungs- und Dokumentationspflicht gemäß Abs. 8 Satz 1 in Höhe von 118,98 EUR (ca. zwei Stunden pro Anwendungsfall einer Analyse für einen PVD der LG 2.1) sowie in Höhe und gleichem Umfang aufgrund der Antragstellung für die richterliche Genehmigung gemäß Satz 4.

- Befugnis zur anlassbezogenen nachträglichen Fernidentifizierung (§ 62b SächsPVDG)

Aufgrund der neuen Regelung in Absatz 1 zum Abgleich von Daten zu Gesichtern und Stimmen mit polizeilichen Systemen entsteht kein zusätzlicher Erfüllungsaufwand, weil die Maßnahme bereits im Polizeialltag vielfach durchgeführt wird und damit Personalaufwand bereits anfällt. Die Befugnis stellt lediglich eine spezifische Rechtsgrundlage für den Abgleich von biometrischen Daten dar, welche den Rückgriff auf die allgemeine Datenverarbeitungsklausel des § 54 Absatz 1 Satz 1 SächsPVDG zukünftig ersetzt.

Kosten für den Personaleinsatz zu einer Analyse nach Absatz 2 (Abgleich biometrischer Daten im Internet) können nur vage geschätzt werden und entstehen für verschiedene Arbeitsabläufe wie die Erstellung der Gefahrenprognose (eine Stunde), die Antragstellung für die richterliche Genehmigung gemäß Absatz 6 Satz 3 (zwei Stunden), die Aufbereitung der Datengrundlagen (zwei Stunden) sowie die Durchführung der Analyse nebst Fertigung des Analyseberichts (zwei Stunden). Unter Zugrundelegung folgender Zeitanteile ergibt sich für einen einfachgelagerten Sachverhalt ein Arbeitsaufwand für einen PVD der LG 2.1 von einem Arbeitstag (ca. 475 EUR) pro Analyse. Schulungskosten hinsichtlich der Analysesoftware entstehen nicht.

Des Weiteren entsteht Erfüllungsaufwand für die nach Satz 5 geregelten Betreiberpflichten bei der Verwendung von Hochrisiko-KI-Systemen gemäß den Vorgaben des Art. 26 KI-VO [Verordnung (EU) 2024/1689]. Danach ist ein Jahresbericht über die Verwendung der genutzten (Analyse)Systemen zu erstellen und den zuständigen Marktüberwachungsbehörden und Datenschutzbehörden vorzulegen. Für die Erstellung eines Jahresberichts ist mit einem Personalaufwand in Höhe von geschätzten 24 Arbeitsstunden für einen Bediensteten der Laufbahngruppe (LG) 2.1 zu rechnen. Dies entspricht ca. 1.427,76 EUR pro Jahr (vgl. Lohnkostentabelle IV. der Anlage 2 zur VwV SächsNKR) Personalkosten.

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

Erforderliche Personalkosten sind fallabhängig und nicht seriös bezifferbar. Je nach Einzelsachverhalt besteht eine unterschiedliche Anzahl von zu überwachenden Telefonanschlüssen und von Gesprächsaufkommen pro Anschluss, welche die Arbeitszeit maßgeblich beeinflusst. Für die Überwachung eines Anschlusses kann an durchschnittlicher Arbeitszeit veranschlagt werden:

Fertigung der Vorlage (eine Stunde) und Erstellung des Antrages für den Behördenleiter zur Beantragung der gerichtlichen Anordnung (zwei Stunden), Umsetzung des Gerichtsbeschlusses und Zustellung an die Telekommunikationsunternehmen (30 Minuten) sowie Überwachung der Telekommunikation des betroffenen Anschlusses für einen Zeitraum von

mindestens 3 Tagen (72 Stunden). Insgesamt entsteht für die Überwachung eines Telefonanschlusses ein Bedarf von insgesamt 76,5 Arbeitsstunden für einen PVD der LG 2.1; dies entspricht Personalkosten in Höhe von ca. 273.059 EUR (vgl. Anlage 2 zur VwV SächsNKR).

Sofern Übersetzungen aus einer ausländischen Sprache erforderlich sind, sind zusätzliche Dolmetscherkosten in Höhe von 65 EUR pro Stunde einzuplanen.

Für das Infiltrieren des Kommunikationsendgerätes (Aufspielen der Software) fällt unterschiedlicher Personalaufwand an. Angestrebt wird der kostenneutrale Einsatz eines sog. Staatstrojaners des BKA. Die Dauer des Aufspielens des Trojaners auf das Endgerät ist abhängig von der Taktik, ob digital oder mit Wechseldatenträger vorgegangen wird. Bei der digitalen Variante dauerte das Aufspielen in bisherigen strafrechtlichen Ermittlungsverfahren im Durchschnitt drei Stunden pro Endgerät; dies würde bei einem Einsatz eines Beamten der LG 2.1 Personalkosten i.H.v. 178,47 EURO gemäß Anlage 2 zur VwV SächsNKR verursachen. Existiert pro Anschluss ein Endgerät, ergäbe dies bei 14 Anschlüssen eine Gesamtsumme i.H.v. 2.498,58 EURO gemäß Anlage 2 zur VwV SächsNKR. Im Falle der Hardware-Variante würde die für die Infiltrierung des Endgerätes zu erbringende Arbeitsleistung unpräzisiert erheblich länger dauern.

Es ist davon auszugehen, dass keine weitere Arbeitszeit für die Überwachungsleistung erforderlich wird, weil ein Mobilfunkanschluss entweder gemäß Absatz 1 oder als Quellen-TKÜ gemäß Absatz 2 überwacht wird. Insofern liegt eine vollumfängliche arbeitszeitliche Kompensation vor.

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

Zusätzliche Kosten für Personal sind nicht zu erwarten, weil Arbeitszeit aufgrund des Wegfalls der bisherigen Arbeitsweise kompensiert werden kann. Es wird lediglich eine Technikart gegen eine andere Technikart ausgetauscht; in allen Einsatzlagen ersetzt das an den Drohnen befestigte luftgestützte Kamerasystem die bislang am Boden eingesetzten Systemen.

- Benachrichtigungs- und Protokollierungspflichten (§§ 74, 75 SächsPVDG)

Aufgrund der Einführung neuer Befugnisse in §§ 57a, 60 (Ermittlungsanfrage), 62a und 62b wird der Katalog der Benachrichtigungspflichten in § 74 und der Protokollierungspflichten in § 75, die zusätzlichen Personalaufwand an Arbeitszeit verursachen, erweitert. Im Fall des § 62a wird aufgrund der erweiterten Protokollierungspflichten gemäß Absatz 9 Satz 2 mit einem zusätzlichen Arbeitsanfall pro Maßnahme in geschätzter Höhe von ca. 15 Minuten gerechnet. Gleiches gilt für die erweiterten Protokollierungspflichten gemäß §§ 57a Abs. 6 Satz 2 und 62b Abs. 7 Satz 2. Im Gegenzug wird durch den Wegfall des § 59 Personalaufwand eingespart. Aussagen über die Anzahl der zu erwartenden Analysen nach den §§ 57a, 62a und 62b und der zu benachrichtigen Personen sind nicht möglich. Allenfalls könnte in Anlehnung an die zuvor geschätzten Fallzahlen davon ausgegangen werden, dass zu allen drei Maßnahmen unter Zugrundelegung eines Arbeitsaufwandes pro Benachrichtigung von ca. 30 Minuten und pro Protokollanfertigung von einer Stunde ca. 300 Arbeitsstunden (17.966 EUR für PVD der LK 2.1 gemäß Anlage 2 der VwV SächsNKR) zusätzlich pro Jahr anfallen werden.

- Befugnis zur Entwicklung, Training und Testen von regelbasierten und lernenden IT-Systemen (§ 79c SächsPVDG)

Zusätzlicher Personalaufwand in geringer Höhe entsteht aufgrund der Einführung einer Dokumentationspflicht in Absatz 1 Satz 7 hinsichtlich der zu verwendeten Daten. Pro Maßnahme ist von einem zusätzlichen Arbeitsanfall in geschätzter Höhe von 30 Minuten auszugehen. Weiterer Erfüllungsaufwand ist nicht zu erwarten, weil Arbeitszeit aufgrund des Wegfalls der bisherigen Arbeitsweise kompensiert werden kann.

- Datenübermittlung an Opferberatungsstellen (§ 84 Abs. 3 Nr. 4 SächsPVDG)

Kosten für den Personaleinsatz beim Polizeivollzugsdienst sind nicht konkret bezifferbar und in Ermangelung einer zentralen Datengrundlage auch nicht recherchierbar. Ausgehend von Erfahrungswerten einer Großstadtdienststelle wären für ganz Sachsen grob geschätzt mit 100 Datenübermittlungen pro Jahr zu rechnen. Dazu wird ein Zeitansatz pro Datenübermittlungsvorgang von maximal 15 Minuten für einen PVD der LG 2.1 angenommen, so dass Personalkosten für 25 Arbeitsstunden i.H.v. 1.487,25 EURO gemäß Anlage 2 zur VwV SächsNKR entstehen würden.

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

Personalkosten entstehen durch die Änderung von Vorlagen, Briefköpfen, Signaturen in E-Mails etc. in Höhe von ca. 875 EUR (35 Stunden x 25 EUR brutto durch Mitarbeiter in E9).

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

Kosten für den Personaleinsatz sind weder bezifferbar noch abschätzbar, weil bereits eine valide Vorhersage zur Anzahl zukünftiger Verstöße und damit Verfahren derzeit nicht möglich ist.

bb) Polizeibehörden

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

cc) Sächsische Datenschutz- und Transparenzbeauftragte

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

dd) Justiz

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

- Datenweiterverarbeitung von durch Bodycam-Einsatz in Wohnungen erlangten Daten (§ 57 Absatz 8 Satz 6)
- besondere Datenverarbeitungsbefugnis im Hinblick auf Daten aus einer Videoüberwachung (§ 57a Absatz 5 Satz 1)
- Verlängerung der Ausschreibung zur verdeckten Beobachtung (§ 60 Absatz 3 Satz

- automatisierte Datenanalysen (§ 62a Absatz 5 und 6)
- biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet (§ 62b Absatz 3 Satz 1)
- Quellen-TKÜ (§§ 66 Absatz 4 Satz 1)

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

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

2) weitere Gesetzesfolgen

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

B. Besonderer Teil

Zu Artikel 1 (Änderung des Sächsischen Polizeivollzugsdienstgesetzes)

Zu Nummer 1

Inhaltsübersicht

Die Änderungen des Inhaltsverzeichnisses ergeben sich aus den nachfolgenden Normanpassungen.

Zu Nummer 2

§ 3

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

Zu Nummer 3

§ 4

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

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

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

Für die in der bisherigen Nummer 7 enthaltene Legaldefinition des „Informationssystems“ besteht kein Regelungsbedarf mehr, da der Begriff im SächsPVDG nicht mehr geführt wird. Die Änderungen in den nunmehrigen Nummern 7 und 8 dienen der Korrektur eines redaktionellen Versehens.

Zu Nummer 4

§ 10

In Nummer 8 wurde das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme neu aufgenommen. Dies erfolgte aufgrund der neu aufgenommenen Befugnis in § 66 Absatz 2 und dem damit verbundenen Grundrechtseingriff.

Zu Nummer 5

§ 12a

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

Während Satz 1 die Abwehrmaßnahmen erst bei Vorliegen einer konkreten Gefahr erlaubt, jedoch bei einer heranfliegenden Drohne der Übergang von einer gefahrlosen Situation hin

zur konkreten Gefahr äußerst kurz erfolgt, ermöglicht Satz 2 ein polizeiliches Handeln bereits im Vorfeld einer konkreten Gefahr, jedoch nicht unmittelbar zur Abwehr dieser Gefahr, sondern zur Erforschung zum Vorliegen einer solchen. Satz 2 setzt damit einen sog. Gefahrenverdacht voraus, der Gefahrerforschungseingriffe ermöglicht, sofern die genannten besonders wichtigen Rechtsgüter bedroht werden können. Zu diesem Zweck kann die Polizei Technik einsetzen, die das Heranfliegen einer Drohne bereits dann detektiert, wenn diese noch räumlich von potentiellen Anschlagzielen oder Aufklärungsorten entfernt ist und noch bevor das menschliche Auge dazu in der Lage ist. Gefahrerforschungsmaßnahmen sind aber nur zum Schutz besonders wichtiger Rechtsgüter zulässig, wenn die Maßnahme weit in das Vorfeld einer Rechtsgutverletzung verlagert wird.

Detektionstechnik kann bspw. zum Scannen des Luftraumes innerhalb eines bestimmten Radius um Kritische Infrastruktur, einer Versammlung/ Ansammlung oder einen gesperrten Luftraum verwendet werden. Die zu verwendende Technik können RF-Systeme, Radar- oder Funkpeilsysteme sowie akustische Sensoren sein.

Satz 3 erlaubt die Maßnahme auch dann, wenn Dritte unvermeidbar betroffen werden. Die Drittbetroffenheit aufgrund einer polizeilichen Interventionsmaßnahme kann dadurch entstehen, dass entweder die eingesetzte Sensortechnik zu Störungen von im Einzugsgebiet des Störsenders befindlichen (Tele-)Kommunikationsgeräten führt oder indem die Drohne unkontrolliert zum Absturz gebracht wird und dadurch Personen- und/oder Sachschäden eintreten können.

Zu Nummer 6

§ 15

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

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

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

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

Zu Nummer 7

§ 19

Die Bekämpfung von häuslicher Gewalt ist eine der polizeilichen Kernaufgaben. Nach dem Bundeslagebild des Bundeskriminalamts zu häuslicher Gewalt für das Kalenderjahr 2023 wurden 256.276 Menschen Opfer solcher Gewalt. Die sogenannte Istanbul-Konvention (Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häusliche Gewalt) verpflichtet Deutschland auf allen staatlichen Ebenen, solcher Gewalt vorzubeugen und sie zu bekämpfen. Zu den staatlichen Schutzinstrumenten gehören auch Maßnahmen nach dem Polizeirecht. Zu diesem Zweck sind ergänzende Regelungen im Sächsischen Polizeivollzugsdienstgesetz vorgesehen (§ 19, § 61, § 84). Durch eine spezifische Befugnisregelung, die sämtliche relevante polizeiliche Standardmaßnahmen beinhaltet, sollen der Polizei klare Maßstäbe an die Hand gegeben werden, damit diese in den besonders eilbedürftigen Situationen Handlungssicherheit hat.

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

Absatz 1

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

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

Nummer 1 beinhaltet die Wohnungsverweisung und das Rückkehrverbot. Nummer 2 a) beinhaltet eine spezifische Befugnisregelung zur Erteilung von Aufenthaltsverboten, die die Regelung des § 21 verdrängt. Nummer 2 b) beinhaltet ein Betretungsverbot für bestimmte Orte, an denen sich die gefährdete Person oder ihr nahestehende Personen (Kinder am Kindergarten oder Schule) aufhalten. Nummer 2 c) regelt das bisher bereits geregelte Kontaktverbot, Nummer 2 d) das Annäherungsverbot. Das Kontaktverbot kann sich auf jede Form der Kommunikation erstrecken. Hierbei ist es irrelevant, ob die Kontaktaufnahme per-

sönlich, schriftlich, unter Vermittlung von Dritten, aber insbesondere auch in der vom Gesetz genannten Form durch Einsatz von (elektronischen) Fernkommunikationsmitteln stattfindet (vgl. BT-Drs. 14/5429 S. 29).

Nummer 2 gilt sowohl für gemeinsam genutzte Wohnungen als auch für eine Wohnung, die ausschließlich durch das Opfer genutzt wird.

In den Sätzen 2 und 3 werden die bestehenden Regelungen zur Befristung des bisherigen Absatz 1 übernommen. In Satz 4 wird der Regelungsinhalt des bisherigen Absatz 3 übernommen. Sollte während der möglichen einmaligen Verlängerung der Maßnahme kein Antrag nach dem Gewaltschutzgesetz gestellt werden, endet die Maßnahme spätestens mit dem Ende des 14. Tages des Anordnungszeitraumes der Verlängerung der Maßnahme.

Zu Nummer 8

§ 21

Absatz 1

Die Neufassung von Satz 1 dient der Klarstellung der Abgrenzung der Anwendungsbereiche von räumlich begrenzten tatortbezogenen Aufenthaltsverboten nach Absatz 1 zu nichttatortbezogenen räumlich weitreichenden Aufenthaltsverboten nach Absatz 2. Für den Erlass eines räumlich begrenzten tatortbezogenen Aufenthaltsverbots nach Absatz 1 ist die Prognose einer Straftatenbegehung durch die betroffene Person an einem bestimmten Ort, in einem bestimmten Gemeindeteil oder einem bestimmten Gemeindegebiet ausreichend. Durch die sprachliche Fassung „bestimmter Ort, ein bestimmtes Gebiet innerhalb einer Gemeinde oder ein Gemeindegebiet“ wird klarstellend die räumlich begrenzte Reichweite eines solchen Aufenthaltsverbots bestimmt. In zeitlicher Hinsicht besteht nach Satz 2 eine Einschränkung dahingehend, dass das Aufenthaltsverbot auf den erforderlichen Umfang zu beschränken ist. Aus Verhältnismäßigkeitsgesichtspunkten wurde jedoch die maximale Anordnungsdauer des bisherigen § 21 Absatz 1 Satz 1 übernommen. Typische Anwendungsfälle für Aufenthaltsverbote nach Absatz 1 sind Gefahren im Zusammenhang mit gewalttätigen Fußballfans oder Drogendealern. Mit den Sätzen 2 und 3 werden die bestehenden Regelungen zum Erfordernis der räumlich/zeitlichen Begrenzung eines Aufenthaltsverbots aus dem bisherigen Absatz 7 übernommen.

Absatz 2

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

Absatz 3

Absatz 3 beinhaltet die bisherige Regelung des Absatzes 4.

Absatz 4

Absatz 4 beinhaltet die bisherige Regelung des Absatzes 5. Zusätzlich wurde klarstellend aufgenommen, dass der Antrag schriftlich gestellt werden muss.

Absatz 5

Absatz 5 beinhaltet die bisherige Regelung des Absatzes 6.

Absatz 6

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

Die Streichung der Absätze 7 und 8 erfolgt in Konsequenz der Änderungen in den Absätzen 1 bis 6.

Zu Nummer 9

§ 28

Die Änderungen erfolgen in Konsequenz von Änderungen in § 15.

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

Zu Nummer 10

§ 29

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

Zu Nummer 11

§ 40

Absatz 4

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

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

Absatz 5

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

Zu Nummer 12

§ 41

§ 41 Absatz 2 Satz 1 bestimmt, dass bei der Anwendung von unmittelbarem Zwang die Bodycam einzuschalten ist. Der neu eingefügte Satz 2 ordnet an, dass wenn der Einsatz von Bodycams in Wohnungen erfolgt, der Maßgabe des Artikels 13 Absatz 7 GG Rechnung zu tragen ist und die Bodycam in Wohnungen zu Dokumentationszwecken bei der Anwendung von unmittelbarem Zwang nur eingeschaltet werden darf, wenn zusätzlich die erforderliche dringende Gefahr für Leib oder Leben der genannten Personen vorliegt. Der neue Satz 3 verweist auf die verfahrensrechtlichen Vorschriften des § 57 Absatz 6 bis 9, die generell für jeden Einsatz einer Bodycam sowohl im Freien als auch in Wohnungen Anwendung finden, unabhängig vom jeweiligen Zweck der Aufzeichnung. Lediglich die Sätze 6 bis 8 des Absatzes 8 (Datenweiterverarbeitung) finden keine entsprechende Anwendung, weil diese auf den Aufzeichnungszweck der Eigensicherung und des Schutzes einer dritten Person in Wohnungen abstellen, § 41 Abs. 2 Satz 2 jedoch gerade nicht diesen Aufzeichnungszwecken dient.

Zu Nummer 13

§ 48

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

Zu Nummer 14

§ 57

Absätze 4 bis 8

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

Absatz 4

Absatz 4 regelt die Anforderungen an das sog. Pre-Recording in Wohnungen. Satz 1 entspricht der bestehenden Regelung in Absatz 4 Satz 1 zum sog. Pre-Recording in öffentlich zugänglichen Bereichen unter Beibehaltung der bisherigen Eingriffsschwelle. Ergänzend wurde zur Klarstellung aufgenommen, im Kontext welcher Aufgabenerfüllung ein Pre-Recording erfolgen kann. Satz 2 beinhaltet neu die Befugnis zum Pre-Recording in Wohnraum mit der Eingriffsschwelle der „dringenden Gefahr“. Satz 3 neu bestimmt im Hinblick auf den weiten Wohnraumbegriff des § 29 Absatz 5 eine Ausnahme von den Anforderungen des Satzes 2. Der Schrankenregelung des Artikel 13 Absatz 7 Grundgesetz (Artikel 30 Absatz 3 Sächsische Verfassung) wurde dadurch Rechnung getragen, dass es sich bei den Rechts-

gütern Leib oder Leben um besonders gewichtige Rechtsgüter handelt. Eine dringende Gefahr liegt vor, wenn eine Sachlage oder ein Verhalten bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens mit hinreichender Wahrscheinlichkeit ein wichtiges Rechtsgut schädigen wird. Hieraus ergibt sich, dass die dringende Gefahr nicht schon eingetreten sein muss.

Absatz 5

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

Absatz 6

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

Satz 2 (neu) enthält im Hinblick auf den Einsatz der Bodycam in Wohnungen und der damit verbundenen möglichen Kernbereichsrelevanz die Verpflichtung zur Unterbrechung von Aufzeichnungen, soweit tatsächliche Anhaltspunkte dafür vorliegen, dass der Kernbereich privater Lebensgestaltung betroffen ist. Satz 2 regelt diesbezüglich, dass die Maßnahme bei erkennbarer Betroffenheit des Kernbereichs privater Lebensgestaltung jedoch erst dann zu unterbrechen ist, wenn dies ohne Gefahr für Leib oder Leben für die eigene oder eine dritte Person möglich ist. Sollte keine Unterbrechung der Aufzeichnung stattfinden, regelt Satz 3 (neu), dass die Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung sowie die Umstände des Fortsetzens der Maßnahme zu dokumentieren sind.

Satz 4 (neu) regelt, wann die Fortsetzung der Maßnahme erfolgen darf. Satz 5 (neu) enthält ein Verwendungsverbot und die Lösungsverpflichtung für Kernbereich-relevante Daten. Satz 6 (neu) bestimmt besondere Dokumentationspflichten, soweit Kernbereichs-relevante Daten erfasst wurden. Satz 7 (neu) regelt eine enge Zweckbeschränkung der Dokumentation nach Satz 6 und bestimmt darüber hinaus die entsprechende Lösfrist.

Absatz 7

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

Absatz 8

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

Satz 2 überführt die Regelung des bisherigen Absatzes 7 Satz 3 und regelt die Lösungsverpflichtung für die nach den Absätzen 4 und 5 erstellten Bild- und Tonaufnahmen sowie die daraus gefertigten Unterlagen. Abweichend hiervon gelten für die Zweckänderung von personenbezogenen Daten aus einem Bodycam-Einsatz in Wohnraum die Anforderungen von Satz 6.

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

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

Satz 6 (neu) regelt, dass die weitere Verarbeitung von in Wohnraum aufgezeichneten Daten nur zulässig ist, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt und keine kernbereichsrelevanten Inhalte aufgezeichnet wurden. Aufgrund der hohen Eingriffstiefe gelten für die Zweckänderung von personenbezogenen Daten aus einem Bodycam-Einsatz in Wohnungen die strengen Anforderungen des § 79a Absatz 4 Satz 1. Für das Verfahren gelten gemäß Satz 7 die Regelungen des Buches 1 des FamFG für entsprechend.

Absatz 9

Absatz 9 entspricht der Regelung des bisherigen Absatz 8.

Absatz 10

Absatz 10 beinhaltet eine geänderte Evaluierungsklausel beschränkt auf den Einsatz von Bodycam in Wohnraum.

Absatz 11

Absatz 11 entspricht der Regelung des bisherigen Absatz 10. Die Löschfrist des Absatz 11 wurde aus Vereinheitlichungsgründen und besserer technischer Praktikabilität auf 30 Tage angepasst.

Absatz 12 entspricht der Regelung des bisherigen Absatz 10.

§ 57a

Anknüpfend an den bestehenden Rechtsrahmen des § 57 Absatz 2 und 3 Sächsisches Polizeivollzugsdienstgesetz, der eine offene Beobachtung und Aufzeichnung von Bilddaten u.a. an Kriminalitätsschwerpunkt-Bereichen oder bei Ansammlungen ermöglicht, soll in Anlehnung an § 14 Absatz 8 HSOG durch eine Befugnis zur „intelligenten Videoüberwachung“ eine vollständige und ausreichend schnelle Auswertung des Bildmaterials ermöglicht werden, um mittels Kontrolle dieser Bereiche Gefahren frühzeitig zu erkennen und hierdurch die Begehung von Straftaten verhindern zu können.

Aufgrund der begrenzten menschlichen Wahrnehmungsfähigkeiten, aber auch aufgrund des erheblichen zeitlichen Aufwandes einer laufenden Auswertung von Bildmaterial soll der Einsatz von Bildanalysesoftware, die automatisiert bestimmte (Bewegungs-)Muster, die auf die Begehung von Straftaten hindeuten, erkennt, gesetzlich geregelt werden. Anknüpfend an eine erfolgte Mustererkennung und Verifizierung einer potentiell gefährlichen Situation durch polizeiliche Bedienstete soll durch die gesetzliche Regelung bei Vorliegen bestimmter deutlich gesteigerter Gefährdungslagen eine biometrische Echtzeit-Fernidentifizierung auf der Grundlage der Datenbestände der polizeilichen Auskunfts- und Fahndungssysteme erfolgen können. Die Erfassung der biometrischen Daten, der Abgleich und die Identifizierung erfolgen nahezu zeitgleich beziehungsweise ohne erhebliche Verzögerung (siehe die Definition Echtzeit- Fernidentifizierungssystem gemäß Artikel 3 Nummer 42 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024-KI-Verordnung).

Darüber hinaus soll angelehnt an § 14 Absatz 9 HSOG daneben eine gesonderte Befugnis zur biometrischen Echtzeit-Fernidentifizierung aufgenommen werden (Absatz 2), um gezielt nach Personen suchen zu können, von denen die konkrete Gefahr oder die vorhersehbare Gefahr einer terroristischen Straftat ausgeht. Weiterer Regelungsbedarf für eine bio-

metrische Echtzeit-Fernidentifizierung besteht für in den polizeilichen Auskunfts- und Fahndungssystemen gespeicherte biometrische Daten von Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie für vermisste Personen.

Flankierend sind in verfahrensrechtlicher Hinsicht Regelungen zum Richtervorbehalt, zu den Anforderungen an die polizeiliche Antragstellung, zur Transparenz, zur aufsichtlichen Kontrolle und zur Gewährleistung effektiven Rechtsschutzes vorgesehen (siehe Ergänzungen in den § 73 ff, 94, § 107 SächsPVDG).

Absatz 1

Der neue § 57a Absatz 1 knüpft in Bezug auf die Zulässigkeit der Datenerhebung an den bestehenden Rechtsrahmen in § 57 Absatz 2 und 3 (u. a. Videoüberwachung an Kriminalitätsschwerpunkten, Ansammlungen) an und ermöglicht den Einsatz intelligenter Bildanalyse-Software nach einer unter Verhältnismäßigkeitserwägungen (zunehmende Eingriffsintensität/höhere Eingriffsschwelle) gestuft gestalteten Datenverarbeitungsbefugnis. Der Einsatz der Bildanalyse-Software darf nicht rückwirkend erfolgen. Dies wird nochmals klargestellt durch die ergänzende Angabe „In Echtzeit“.

Satz 1 regelt die erste Stufe und erlaubt den Einsatz von Bildanalyse-Software bzw. intelligenter Videoüberwachung zur Erkennung von Mustern von auf der Grundlage von § 57 Absatz 2 und 3 rechtmäßig erhobenen personenbezogenen Daten in Echtzeit. Satz 2 ordnet bei Mustererkennung durch die Bildanalyse-Software an, dass durch Polizeibedienstete die Prüfung eines erkannten Musters zu erfolgen hat und ob mit Straftaten von erheblicher Bedeutung in absehbarer Zeit mit hinreichender Wahrscheinlichkeit gerechnet werden kann. Satz 3 regelt die zweite Stufe der Datenverarbeitung und erlaubt die Nachverfolgung nur solcher Personen, die eine Gefahr nach Satz 2 verursachen. Satz 4 regelt die dritte und letzte Stufe und erlaubt die biometrische Echtzeit-Fernidentifizierung. Die Befugnisregelungen der Sätze 2 und 3 stellen dabei sicher, dass die Auswertung von Trefferfällen nicht automatisiert, sondern durch den Menschen erfolgt.

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

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

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

Wesensmerkmal der eingesetzten Technik ist ein bereits austrainiertes und ausgelerntes System, das die einzelnen Bildaufzeichnungen in Echtzeit auswertet und dadurch auffällige Bewegungsmuster aufspüren bzw. kenntlich machen kann. Die verwendeten KI-Modelle werden von dem jeweiligen Anbieter trainiert und sind als solche unveränderlich vorprogrammiert, d. h. die eingesetzten Modelle lernen nicht auf Grundlage der polizeilichen Daten weiter (siehe Absatz 6). Eine Verknüpfung oder ein Abgleich mit gespeicherten Daten findet nicht statt. Es werden lediglich tatsächliche Geschehensabläufe mit abstrakten Bewegungsmustern abgeglichen, um ein polizeilich relevantes Verhalten zu identifizieren. Personenbezogene Daten sind daher nicht bzw. nur in einem sehr geringfügigen Umfang betroffen. Durch die Mustererkennung erfolgt zwar eine quantitative Steigerung der Datenverarbeitung, die, da die Auswertung aber nicht auf der Grundlage personenbezogener Merkmale erfolgt, jedoch nicht eingriffsintensiver ist, als die Datenerfassung im Vergleich zur konventionellen Videoüberwachung.

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

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

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

Absatz 2

Durch die Regelung in Satz 1 wird eine – neben der Regelung des Absatzes 1 stehende - spezifische Befugnis zum Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme zur gezielten Suche nach Personen, die eine bestehende oder vorhersehbare Gefahr durch die Begehung einer terroristischen Straftat verursachen, in das Sächsische Polizeivollzugsdienstgesetz aufgenommen. Die Regelung orientiert sich eng an dem von Artikel 5 Absatz 1

Ziffer h) ii) der KI-VO gesetzten Regelungsrahmen. Satz 2 enthält eine spezifische Befugnisregelung zum Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme zur gezielten Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung oder von vermissten Personen. Auch diese Befugnisregelung hält den durch Artikel 5 Absatz 1 Ziffer h) i) KI-VO gesetzten Regelungsrahmen ein und greift deren Wortlaut auf. Ein Abgleich der erhobenen Daten darf nur mit Daten erfolgen, die durch Maßnahmen nach § 57 Absatz 2 und 3 erhoben wurden. Die Befugnisse nach Satz 1 und 2 dürfen nur dann angewandt werden, wenn die Suche nach den Personen auf diese Weise unbedingt erforderlich ist. Satz 2 sichert im Hinblick auf die vom Sächsischen Verfassungsgerichtshof durch Urteil vom 25. Januar 2024, Vf. 91-II-19, Seite 54, erfolgte Rechtsprechung zur gesetzgeberischen Gestaltung von Eingriffsschwellen im Vorfeld von Gefahren, die Einhaltung der verfassungsrechtlich geforderten Eingriffsschwelle.

Absatz 3

Die Regelung in Satz 1 beinhaltet besondere Anforderungen zur Gewährleistung des Grundsatzes der Verhältnismäßigkeit. Sie stellt sicher, dass bei jeglicher Maßnahme nach Absatz 1 Satz 1 (Mustererkennung), Satz 3 (Nachverfolgung) und Satz 4 (Echtzeit-Identifizierung im Stufenverhältnis), als auch bei Maßnahmen nach Absatz 2 (gezielte Echtzeit-Identifizierung) der Anforderung der Begrenzung auf das im jeweiligen Einzelfall geforderte zeitliche und örtliche Maß eingehalten wird. Damit wird gesetzlich eine besondere Prüfung und strenge Beschränkung der jeweiligen Maßnahme sowohl in zeitlicher (Dauer) als auch in örtlicher Hinsicht somit im Hinblick auf den räumlich erforderlichen Bereich, angeordnet.

Satz 2 stellt sicher, dass sich die Echtzeit-Fernidentifizierung nur gegen solche Personen richtet, deren biometrische Daten im Rahmen der Regelung des Absatzes 1 Satz 4 oder des Absatzes 2 abgeglichen werden dürfen. Das sind nur Personen, von denen die Gefahr für die Begehung der betreffenden Straftaten ausgeht oder Personen, bei denen von Gefährdungen für hochrangige Rechtsgüter auszugehen ist.

Absatz 4

Satz 1 beinhaltet eine strikte Zweckbindung der verarbeiteten biometrischen Daten. Der Ausschluss der Geltung von § 79a sichert, dass diese Daten weder zu einem anderen Zweck verarbeitet noch zweckkonform genutzt werden dürfen (Satz 2). Die Regelung in Satz 3 stellt sicher, dass nicht allein auf der Grundlage des Ergebnisses des Abgleichs polizeiliche Folgemaßnahmen getroffen werden können und dient damit der Eingrenzung der Beeinträchtigung von Unbeteiligten. Weitere polizeiliche Maßnahmen setzen voraus, dass zunächst eine Prüfung und Bestätigung des Ergebnisses des Abgleichs durch Polizeibedienstete erfolgt. Satz 4 erlaubt die Speicherung des Abgleichsergebnisses und der zur Durchführung des Abgleichs erhobenen Daten erst dann, wenn die Prüfung nach Satz 3 durch Polizeibedienstete dazu geführt hat, dass weitere polizeiliche Maßnahmen erforderlich sind. Anderenfalls sind nach Satz 5 alle Daten technisch spurlos und automatisiert zu löschen und dürfen nicht verarbeitet werden. Satz 6 sieht eine technisch spurlose und automatisierte Löschung ebenfalls für den Fall vor, dass keine Datenübereinstimmung nach Satz 3 vorliegt.

Absatz 5

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

hördenleiter vorbehalten (Satz 1 und 3). Satz 4 bestimmt, dass (abweichend von § 73 Absatz 3 Satz 3) für Anordnungen von Maßnahmen der gezielten Echtzeit- Fernidentifizierung nach Absatz 2 Satz 1 eine Höchstanordnungsdauer von sieben Tagen gilt. Diese kann um den gleichen Zeitraum verlängert werden, wenn die Anordnungsvoraussetzungen weiterhin vorliegen (Sätze 5 und 6).

Ergänzend gelten die Regelungen über die Anordnung und gerichtliche Zuständigkeit in § 73. Über § 73 Absatz 3 besteht das Schriftformerfordernis für die richterliche Anordnung und für die polizeiliche Anordnung bei Gefahr im Verzug (§ 73 Absatz 5).

Absatz 6

Satz 1 trifft Vorkehrungen zum Grundrechtsschutz, indem gesetzlich angeordnet wird, dass sicherzustellen ist, dass nur bestimmte qualifizierte Polizeibedienstete, somit in besonderer Weise geschulte Polizeibedienstete, die automatisierten Systeme anwenden dürfen.

Satz 2 sichert durch die § 75 ergänzende Regelung zur vollständigen Protokollierung der Maßnahme und der Protokollierungspflicht, welche oder welcher Polizeibedienstete die Maßnahme angewendet hat, die Transparenz polizeilichen Handelns und andererseits die nachträgliche aufsichtliche Kontrolle. Die Regelung dient zudem zusammen mit der Benachrichtigungspflicht nach § 74 Absatz 1 Nummer 1 auch der Gewährleistung effektiven Rechtsschutzes.

Satz 3 ordnet die Anforderung der Nachvollziehbarkeit des jeweils zur Datenverarbeitung eingesetzten Verfahrens zum Zweck der Gewährleistung von Rechtsschutz und aufsichtlicher Kontrolle sowie der Sicherstellung, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden, an.

Durch die in Satz 4 geregelte Verpflichtung, die oder den Sächsische(n) Datenschutz- und Transparenzbeauftragte(n) über abgeschlossene Maßnahmen nach Absatz 1 Satz 4 und Absatz 2 zu informieren, wird die Möglichkeit einer aufsichtlichen Kontrolle eröffnet und damit die Möglichkeit der Darstellung im jährlichen Bericht gewährleistet.

Satz 5 stellt klar, dass § 94 trotz der Informationspflicht an die oder den Sächsische(n) Datenschutz- und Transparenzbeauftragte(n) unberührt bleibt.

Satz 6 bestimmt, dass bei Maßnahmen nach Absatz 1 Satz 1, 3 oder 4 oder Absatz 4 und somit bei der Anwendung von automatisierten Systemen zum Echtzeit-Abgleich, der Einsatz selbstlernender Systeme ausgeschlossen ist.

Satz 7, 8 und 9 dienen der Umsetzung der jeweiligen Pflichten der Artikel 5 und 26 der KI-VO.

Absatz 7

Das Bundesverfassungsgericht gestattet es dem Gesetzgeber, benötigte technisch-organisatorische Regelungen zur Milderung der Eingriffsintensität von Befugnissen bei besonderer Technizität oder rascher Fortentwicklungsmöglichkeit an die Verwaltung zu delegieren.

Mit Absatz 7 wird von der Delegationsmöglichkeit Gebrauch gemacht und das Sächsische Staatsministerium des Innern beauftragt, das Nähere zum Verfahren, insbesondere unter Berücksichtigung der gesetzlich angeordneten Regelungsinhalte, in einer Rechtsverordnung zu bestimmen. In den Nummern 1 bis 5 werden die zu regelnden Inhalte benannt.

§ 58

In Umsetzung der Rechtsprechung des Bundesverfassungsgerichts zu Kfz-Kennzeichenkontrollen in Bayern, Baden-Württemberg und Hessen (Beschluss vom 18. Dezember 2018

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

Absatz 1

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

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

Absatz 2

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

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

Absatz 3

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

Absatz 4

Die Regelung entspricht der Bisherigen in Absatz 3 Satz 1.

Absatz 5

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

Absatz 6

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

Zu Nummer 15

§ 59

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

Zu Nummer 16

§ 60

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

Absatz 1

In Satz 1 wird die „Ermittlungsanfrage“ als weiterer Ausschreibungsgrund aufgenommen und zugleich für sämtliche Ausschreibungen eine einheitliche Befugnissschwelle bestimmt. Die Ausschreibung zur verdeckten Kontrolle stellt als Maßnahme, die der betroffenen Person nicht bekannt wird, eine Grundrechts-intensivere Maßnahme gegenüber den Ausschreibungen der gezielten Kontrolle oder der Ermittlungsanfrage dar, da letztere der betroffenen Person bekannt werden. Gleichwohl sah die bisherige Regelung für die Befugnis der gezielten Kontrolle eine höhere Eingriffsschwelle als für die verdeckte Kontrolle vor. Mit

der Regelung einer einheitlichen Eingriffsschwelle für sämtliche Ausschreibungsarten wird dies korrigiert. Die bisherige Regelung zur Befugnis zur Ausschreibung von Kontakt- und Begleitpersonen wird aus Gründen der Verhältnismäßigkeit gestrichen.

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

Absatz 2

Mit den Änderungen in Absatz 2 werden die im Fall eines Antreffens einer ausgeschriebenen Person oder Sache zulässigen Anschlussbefugnisse unter Berücksichtigung des neu aufgenommenen Ausschreibungsgrundes der „Ermittlungsanfrage“, unterscheidend nach Art der Ausschreibung, gesetzlich bestimmt. Nummer 1 beinhaltet die bisherige Regelung des § 60 Absatz 4 Satz 1, Nummer 2 beinhaltet die bisherige Regelung des § 60 Absatz 4 Satz 2 und präzisiert diese. Mit der Regelung in Nummer 3 wird im Hinblick auf den Ausschreibungsgrund der Ermittlungsanfrage klarstellend auf die Befugnis der Befragung verwiesen.

Absatz 3

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

Absatz 4

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

§ 61

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

Absatz 1

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

Absatz 2

In Absatz 2 wird der Regelungsinhalt des bisherigen § 61 Absatz 3 übernommen (siehe Sätze 1, 3 bis 6). Zur Klarstellung wurde in Satz 2 eine Regelung zur Erstellung eines Bewegungsbildes aufgenommen. Die Erstellung eines solchen ist nunmehr zulässig, wenn

ersichtlich ist, dass die elektronische Aufenthaltsüberwachung nur dann ihren Zweck erfüllen kann, wenn die Bewegungsdaten des Betroffenen zu einem Bewegungsbild verbunden werden. Satz 3 sieht vor, dass im häuslichen Umfeld der betroffenen Person keine Daten erhoben werden können, die über den bloßen Umstand deren Anwesenheit hinausgehen.

Durch technische Mittel, welche in der Wohnung des Betroffenen installiert werden, wird hierbei sichergestellt, dass das GPS-Signal unterdrückt wird, solange sich der Betroffene in diesem Bereich befindet. Die zulässigen Verwendungszwecke von nach Satz 1 und 2 erhobenen Daten werden durch die in Satz 7 angepassten Regelungen zur Zweckbindung bzw. im Rahmen der Zweckänderung mit Anpassungen bestimmt. Satz 8 (neu) setzt die Vorgaben des Urteils des Sächsischen Verfassungsgerichtshofs um.

Absatz 3

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

Absatz 4

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

Absatz 5

In Absatz 5 wurde der Regelungsinhalt des bisherigen § 61 Absatz 7 Satz 1 und 2 übernommen.

Absatz 6

Absatz 6 Satz 1 (neu) bestimmt, dass auf Antrag der Polizei die Erstellung eines Bewegungsbildes nur dann zulässig ist, wenn dies durch richterliche Anordnung ausdrücklich gestattet ist. Eine Ausnahme des Erfordernisses zur Einholung einer richterlichen Anordnung besteht lediglich bei Anordnungen nach Absatz 1 Nummer 3. Die Sätze 2 bis 4 beinhalten die Regelungen des bisherigen § 61 Absatz 8 Sätze 1 bis 3.

Absatz 7

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

Zu Nummer 17

§ 62a

Mit der neu aufgenommenen Regelung in § 62a wird die Polizei in die Lage versetzt, bereits vorhandene Informationen einfacher, schneller und wirksamer aus Anlass einer erforderlichen Einzelfallbearbeitung auszuwerten. Die neue Befugnis führt drei Maßnahmen zur Weiterverarbeitung vorhandener personenbezogener Daten ein: den niederschweligen besonderen automatisierten Datenabgleich (Absatz 1), die automatisierte regelbasierte Datenanalyse mit eingeschränktem Eingriffsgewicht (Absatz 2) und die automatisierte Datenanalyse unter Einsatz von selbstlernender KI (Absatz 5).

Mit der Regelung in Absatz 1 wird der Anforderung des Sächsischen Verfassungsgerichtshofs nachgekommen, dass jede Datenverarbeitung, die über einen einfachen Datenabgleich hinausgeht, einer spezifischen Rechtsgrundlage bedarf. Der Sächsische Verfassungsgerichtshof hat in seinem Urteil vom 25. Januar 2024 darauf verwiesen, dass die Re-

gelung des § 80 Absatz 1 SächsPVDG nicht zu automatisierten Datenanalysen oder -auswertungen ermächtigt, die über ein automatisiertes Abrufverfahren nach § 85 hinausgehen (siehe Urteil a. a. O., Seite 118 letzter Absatz).

Mit den neuen Befugnissen in den Absätzen 2 und 5 wird die durch die getrennten polizeilichen Datenbestände erschwerte umfassende Auswertung polizeilich zu bearbeitender Sachverhalte überwunden. Die informationstechnische Entwicklung der letzten Jahre ermöglicht es, bisher unverbundene automatisierte Dateien und Datenquellen auf einer Analyseplattform zusammenzuführen und die vorhandenen Datenbestände durch Suchfunktionen systematisch zu erschließen. Hierdurch können über die bisherigen Erkenntnismöglichkeiten hinaus Zusammenhänge (zum Beispiel Handlungsmuster zwischen verschiedenen Personen oder Personengruppierungen), erkannt und dadurch die Wirksamkeit der vorbeugenden Straftatenbekämpfung gesteigert werden. In seinem Urteil vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20) hat das Bundesverfassungsgericht die Überwindung der bestehenden Erkenntnisgrenzen in der polizeilichen Praxis durch automatisierte Datenanalyse als zulässig erkannt und dargelegt, unter welchen Voraussetzungen eine automatisierte Datenanalyse mit graduellen Abstufungen und daher unterschiedlichem Eingriffsgewicht verfassungskonform geregelt werden kann. Die Verarbeitung gespeicherter personenbezogener Daten im Rahmen einer automatisierten Datenanalyse greift in das Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG in zweifacher Weise ein. Zum einen stellt die Nutzung der Daten über den ursprünglichen Anlass hinaus einen neuen Grundrechtseingriff dar, der nach dem Grundsatz der Zweckbindung gerechtfertigt sein muss. Zum anderen hat das Bundesverfassungsgericht in der bezeichneten Entscheidung der automatisierten Datenanalyse ein besonderes Eigengewicht zugewiesen, das über das Eingriffsgewicht der weiteren Verwendung vormals getrennter Daten hinausgeht (BVerfG, a. a. O., Rz. 50, 67 ff.).

Für eine verfassungskonforme Ausgestaltung der automatisierten Datenanalyse ist eine Bestimmung dieses Eigengewichts erforderlich, das je nach Art und Umfang der einzubeziehenden Daten und der Methode der Analyse sehr unterschiedlich sein kann (BVerfG, a. a. O., Rz. 72 ff.). Die gesetzlichen Anforderungen für eine verfassungskonforme Regelung der Eingriffsschwellen bestimmen sich daher nach dem jeweiligen Eingriffsgewicht der automatisierten Datenanalyse und deren Gestaltung durch eingriffsminimierende Vorkehrungen und Schutzmaßnahmen.

Mit Absatz 2 wird die Befugnis zur automatisierten Datenanalyse nach vordefinierten Regeln eröffnet. Der Analysevorgang hat daher einem klar definierten, unveränderlichen Ablauf zu folgen, der der Nachvollziehbarkeit unterliegt. Durch Absatz 5 wird für den Analysevorgang der Einsatz selbstlernender Systeme in eng umgrenztem Anwendungsbereich eröffnet.

Mit den vorgesehenen Regelungen werden der Polizei zum Zweck der Unterstützung der polizeilichen Aufgabenerfüllung unterschiedlich eingriffsintensive automatisierte Datenverarbeitungsbefugnisse mit gestuften Eingriffsschwellen zur Verfügung gestellt und damit eröffnet neue Erkenntnisse zu gewinnen, die ihr die notwendigen Bewertungen, Prognosen und Entscheidungen zur Abwehr von Gefahren und bevorstehenden Straftaten ermöglichen.

In Absatz 3 wird die Methode der automatisierten Datenanalyse nach Absatz 2 und 3 bestimmt. Absatz 4 regelt, welche Datenquellen bzw. welche Daten einem besonderen automatisierten Datenabgleich oder einer automatisierten Datenanalyse zugeführt werden dürfen bzw. welche Daten hiervon ausgeschlossen sind. Absatz 6 regelt die spezifischen Anforderungen, die für die Erstellung eines Verhaltensprofils gelten. Absatz 7 bestimmt die Zulässigkeit der Speicherdauer der für die automatisierte Datenanalyse zusammengeführten Datenbestände und ordnet an, wann diese zu löschen sind. Absatz 8 regelt schließlich

entsprechend dem unterschiedlichen Eingriffsgewicht der Maßnahmen die Anordnungsbefugnisse. Absatz 9 beinhaltet verfahrensrechtliche Bestimmungen, die dem Grundrechtsschutz, der Gewährleistung von Rechtsschutz und aufsichtlicher Kontrolle dienen.

Absatz 1

In Absatz 1 wird die neue Befugnis zum besonderen automatisierten Datenabgleich eingeführt. Es handelt sich hierbei um eine Maßnahme mit geringem Eingriffsgewicht. Gestattet sind hierbei nur regelbasierte Systeme. Die Befugnis soll der Polizei die Möglichkeit eröffnen, im Zusammenhang mit der Bearbeitung eines konkreten Sachverhalts entsprechend eingegebener Suchkriterien Übereinstimmungen zwischen Daten aus einer zuvor händisch einbezogenen begrenzten Anzahl von Vorgängen zu erzielen. Im Unterschied zum einfachen Datenabgleich nach § 87 SächsPVDG, dessen Zweck darin besteht, Kenntnis zu erlangen, ob zu einer bestimmten Person Erkenntnisse in den polizeilichen Datensystemen gespeichert sind, stellt die neue Befugnis des besonderen automatisierten Datenabgleichs ein Instrument dar, das der Polizei eine gezielte Suche nach Übereinstimmungen von Daten und damit des Erkennens von Beziehungen zwischen Daten aus einem überschaubaren Datenbestand ermöglicht (Satz 1).

Satz 2 ordnet an, dass in den besonderen automatisierten Datenabgleich nur solche Daten einbezogen werden können, die zuvor durch gezielte Abfragen und somit „händisch“ zusammengeführt wurden.

Absatz 2

Absatz 2 regelt die neue Befugnis zum automatisierten Abgleich mittels regelbasierter automatisierter Datenanalyse. Hierbei handelt es sich um eine Befugnis, der ein deutlich höheres Eingriffsgewicht als dem besonderen automatisierten Datenabgleich zukommt. Das technische Verfahren einer automatisierten Datenanalyse besteht aus zwei aufeinander aufbauenden Schritten, nämlich dem automatisierten Zusammenführen von Daten aus unterschiedlichen Dateisystemen und der sich daran anschließenden Recherche innerhalb der zusammengeführten Datenbestände und deren automatisierter regelbasierter Analyse, die dem Zweck der Gewinnung neuer Erkenntnisse dient. Mit dem automatisierten Zusammenführen wird das strukturelle Problem, dass in den Beständen der Polizei Daten in unterschiedlichen Formaten und getrennten Dateien gespeichert sind, und damit nicht im selben Bearbeitungskontext gleichzeitig verfügbar sind, behoben. Daran knüpft die regelbasierte automatisierte Datenanalyse, die in einer Verknüpfung, Aufbereitung und Auswertung der zusammengeführten Datenbestände besteht, an.

Mit der Verweisung auf § 79a wird klargestellt, dass eine Weiterverarbeitung im Rahmen der automatisierten Datenanalyse nur nach Maßgabe der Grundsätze der Zweckbindung und Zweckänderung erfolgen darf. Die Datenanalyse wird zudem auf die in Absatz 4 abschließend bezeichneten Datenquellen beschränkt. Ausgeschlossen sind Daten aus bestimmten eingriffsintensiven Befugnissen (beispielsweise Wohnraumüberwachung). Weiterhin ausgeschlossen sind biometrische Daten und Daten von Unbeteiligten aus der Vorgangsbearbeitung. Wesentlich eingriffsminimierend wirkt zudem die gesetzliche Anordnung, dass die automatisierte Datenanalyse nur auf der Grundlage anlassbezogener Suchkriterien erfolgen darf. Diesem Eingriffsgewicht wird bei der Gestaltung der Eingriffsschwellen durch den Rang der zu schützenden Rechtsgüter und bei der Anforderung an die zeitliche Nähe des drohenden Schadens Rechnung getragen.

Satz 1 regelt in den Nummern 1 bis 3 drei unterschiedliche Eingriffsschwellen, die jeweils Anlass für eine automatisierte regelbasierte Datenanalyse sein können.

Die Eingriffsschwelle in Nummer 1 setzt das Vorliegen einer konkreten Gefahr (siehe Begriffsbestimmung in § 4 Nummer 3a SächsPVDG) für besonders gewichtige Rechtsgüter voraus. Da der Eingriffsanlass mit dem Erfordernis einer konkreten Gefahr streng begrenzt ist und hohe Anforderungen an die zu schützenden Rechtsgüter gestellt werden (es muss

sich um besonders gewichtige Rechtsgüter handeln), zudem ein Angriff von erheblicher Intensität drohen und die Datenanalyse erforderlich sein muss, um einen Schaden von den Rechtsgütern abzuwenden, darf das Eingriffsgewicht der automatisierten regelbasierten Datenanalyse unter diesen Voraussetzungen vergleichsweise hoch sein.

Die Eingriffsschwelle in Nummer 2 lässt das Vorliegen einer konkretisierten Gefahr für die Begehung einer zumindest ihrer Art nach konkretisierten Straftat von erheblicher Bedeutung genügen, wenn sie sich gegen ein besonders gewichtiges Rechtsgut (siehe Nummer 1) richtet. Eine hinreichend konkretisierte Gefahr kann schon vorliegen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, jedoch bereits bestimmte Tatsachen darauf hinweisen, dass eine entsprechende Straftat begangen werden wird. Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (BVerfG, a. a. O., Rz. 106).

Die Eingriffsschwelle in Nummer 3 regelt das Gefahrenvorfeld und bleibt somit hinter einer konkretisierten Gefahr zurück. Zur Wahrung der Verhältnismäßigkeit wird als Schwelle die Begehung einer terroristischen Straftat und demnach der Schutz besonders gewichtiger Rechtsgüter bestimmt. Satz 2 setzt die Rechtsprechung des Sächsischen Verfassungsgerichtshofs um, wenn es sich bei der in Bezug genommenen Straftat um eine Vorfeldstraftat handelt.

Absatz 3

Absatz 3 stellt klar, dass es sich bei der automatisierten Datenanalyse lediglich um ein technisches Hilfsmittel handeln darf, das die bisherige Arbeitsweise der Polizei erleichtert, ohne sie grundlegend zu verändern.

Satz 1 sichert die Funktion der automatisierten Datenanalyse als bloßes Hilfsmittel für die polizeiliche Aufgabenwahrnehmung ab, indem klargestellt wird, dass die automatisierte Datenanalyse manuell auf der Grundlage von anlassbezogenen Suchkriterien auszulösen ist.

Aus der Entscheidung des Bundesverfassungsgerichts folgt, dass das Eingriffsgewicht der automatisierten Datenanalyse umso höher ist, je offener die Methode des Suchvorgangs gestaltet ist (BVerfG, a. a. O., Rz. 93).

Diese gesetzlichen Vorgaben dienen der weiteren Eingriffsminimierung. Die mit einer offenen Suche verbundenen Gefahren können durch eine Einschränkung der Datenverarbeitungsmethode gesenkt werden, wenn der Suchvorgang eingrenzend so geregelt ist, dass er einen Bezug zu einem konkreten Suchanlass voraussetzt (BVerfG, a. a. O., Rz. 95). Indem in Satz 1 geregelt wird, dass die automatisierte Datenanalyse anhand von „Suchbegriffen“ zu erfolgen hat, die sich auf einen Anlass im Sinne des Absatzes 2 Satz 1 stützen müssen, wird eine sachliche Verbindung zwischen dem gefährdeten Rechtsgut und den von automatisierten Anwendungen betroffenen Personen vorausgesetzt.

Satz 2 ordnet an, dass der Suchvorgang vorrangig an den Personen ansetzen hat, die für die Gefahr verantwortlich sind. Der Suchvorgang der automatisierten Datenanalyse kann, wenn eine Ausrichtung auf die Person, die im Anlassfall Gefahrenverantwortlicher ist, nicht zu den erforderlichen Erkenntnissen geführt hat oder nachvollziehbar nicht führen wird, an einer Person ansetzen, die im betreffenden Anlassfall nicht Gefahrenverantwortlicher ist. Durch die Regelung des Absatz 3 Satz 1 ist jedoch für die Zulässigkeit einer automatisierten Datenanalyse auch insoweit Voraussetzung, dass bei dieser Person ein konkreter Bezug zu dem konkreten Gefährdungssachverhalt besteht, der den jeweiligen gesetzlich geregelten Anlassfall für den automatisierten Datenabgleich bildet. Die automatisierte Datenanalyse darf keine Prognosesoftware in dem Sinne sein, dass sie eigenständig kriminelles Ver-

halten vorhersagt und die von einem Menschen zu treffende Sachverhaltsbewertung ersetzt. Sie darf lediglich ein technisches Hilfsmittel sein, das die Polizei bei ihrer Aufgabewahrnehmung unterstützt, indem sie Informationen aus verschiedenen Dateisystemen zum Zweck der Gewinnung neuer Erkenntnisse zusammenführt. Die abschließende Bewertung der zusammengeführten Informationen und gewonnenen Erkenntnisse bleibt Aufgabe der Bediensteten der Polizei.

Satz 3 bestimmt, dass abschließende maschinelle Sachverhaltsbewertungen verboten sind. Die abschließende Bewertung der durch die automatisierte Datenanalyse bereitgestellten Informationen und die Entscheidung über die auf der Grundlage der bereitgestellten Informationen zu treffenden weiteren Maßnahmen verbleiben bei den Bediensteten der Polizei.

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

Absatz 4

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

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

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

Mit dem Begriff der Verkehrsdaten werden gemäß der Legaldefinition in § 3 Nummer 70 TKG diejenigen Daten erfasst, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind. Hierzu gehören insbesondere

auch die für die Polizeiarbeit praktisch bedeutsamen Standortdaten (vgl. § 9 Absatz 1 Nummer 1 TDDDG), die repressiv oder präventiv unter den jeweiligen gesetzlichen Anforderungen erhoben werden können. Die Kenntnis darüber, welches mobile Telekommunikationsendgerät zu einem bestimmten Zeitpunkt an einem bestimmten Ort angemeldet war, kann für die polizeiliche Ermittlungsarbeit von wesentlicher Bedeutung sein, weil der Aufenthaltsort der Anschlussinhaberin oder des Anschlussinhabers zum Beispiel Aufschlüsse über Organisationsstrukturen einer Mehrheit von Tatverdächtigen geben kann.

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

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

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

Satz 3 enthält ein ausdrückliches Verbot der direkten Anbindung der Analyseplattform an Internetdienste und minimiert durch die Begrenzung der Daten, die einbezogen werden dürfen, das Eingriffsgewicht.

Satz 4 ordnet zur Gewährleistung des Grundsatzes der Zweckbindung und Zweckänderung an, dass nur gekennzeichnete Daten (§ 81 SächsPVDG) durch besonderen automatisierten Datenabgleich oder automatisierte Datenanalyse weiterverarbeitet werden dürfen.

Gemäß Satz 5 Nummer 1 dürfen personenbezogene Vorgangsdaten Unbeteiligter nicht in die automatisierte Datenanalyse einbezogen werden. Nummer 2 schließt Daten aus der Wohnraumüberwachung und gemäß § 79a Absatz 4 Satz 3 erlangte Daten sowie Daten aus dem Bodycam-Einsatz in Wohnungen aus. Nummer 3 verbietet schließlich die Einbeziehung von biometrischen Daten in die automatisierte Datenanalyse.

Satz 6 ordnet an, dass für den automatisierten besonderen Datenabgleich der Ausschluss der in Satz 5 Nummern 2 und 3 bezeichneten Daten gilt. Einbezogen sein dürfen insoweit jedoch jegliche Vorgangsdaten.

Mit Satz 7 wird schließlich eine weitere eingriffsbeschränkende Regelung bei der automatisierten Datenanalyse nach Absatz 2 Nummer 3 (Verhalten der Person begründet die konkrete Wahrscheinlichkeit der Begehung einer terroristischen Straftat) getroffen, indem die Einbeziehung von Verkehrsdaten aus Funkzellenabfragen ausgeschlossen wird. Der Ausschluss erfolgt aufgrund Verhältnismäßigkeitsabwägungen vor dem Hintergrund der potentiell hohen Zahl Unbeteiligter.

Absatz 5

Aufgrund der voranschreitenden technologischen Entwicklungen ist es zur Gewährleistung einer effizienten Gefahrenabwehr erforderlich, den möglichen Rechtsrahmen auszuschöpfen und der Polizei auch die Anwendung selbstlernender Systeme bei der automatisierten Datenanalyse unter Berücksichtigung der verfassungsrechtlichen Anforderungen und der Anforderungen der KI-VO zu eröffnen. Dem hohen Eingriffsgewicht einer solchen Befugnis wird durch die in Satz 1 bestimmten Eingriffsschwellen und begleitenden verfahrensrechtlichen Anforderungen Rechnung getragen. Eine automatisierte Datenanalyse unter Einsatz von selbstlernenden Systemen wird dabei allein in den Anwendungsvarianten der konkreten Gefahr für hochrangige Rechtsgüter (Absatz 2 Satz 1 Nummer 1) oder der konkretisierten Gefahr der Begehung von besonders schweren Straftaten nach § 100b Absatz 2 StPO, die sich gegen die in Absatz 2 Satz 1 Nummer 1 genannten Rechtsgüter richten, bzw. von terroristischen Straftaten zugelassen. Durch Nummer 2 ordnet der Gesetzgeber an, dass die Maßnahme zur Verhütung der Straftat erforderlich sein muss. Mit diesen hohen Eingriffsschwellen wird dem Eingriffsgewicht dieser Art der Datenanalyse Rechnung getragen. Satz 2 setzt die Rechtsprechung des Sächsischen Verfassungsgerichtshofs um, wenn es sich bei der in Bezug genommenen Straftat um eine Vorfeldstraftat handelt.

Absatz 6

Satz 1 bestimmt die spezifischen Anforderungen unter denen mittels automatisierter Datenanalyse nach Absatz 2 das Verhalten einer Person für einen begrenzten Zeitraum nachvollziehbar gemacht werden kann.

Satz 2 beschränkt den Zeitraum, auf den sich ein Verhaltensprofil beziehen darf, auf eine Woche. Durch die Verweisung auf eine automatisierte Datenanalyse nach Absatz 2 ist der Einsatz selbstlernender Systeme ausgeschlossen.

Absatz 7

Satz 1 bestimmt zum Zweck der Grundrechtssicherung die Zulässigkeit der Speicherdauer der für die automatisierte Datenanalyse zusammengeführten Daten. Diese dürfen nur solange gespeichert werden, wie dies für den jeweiligen Zweck der automatisierten Datenanalyse nach Absatz 2, 5 oder 6 erforderlich ist.

Satz 2 ordnet daher die unverzügliche Löschung des für die Datenanalyse zusammengeführten Datenbestandes an, wenn sich hieraus keine neuen Erkenntnisse ergeben oder die weitere Speicherung für den der automatisierten Datenanalyse zugrundeliegenden Zweck nicht mehr erforderlich ist.

Zur Absicherung der Löschungsverpflichtung nach Satz 2 verpflichtet Satz 3 die Polizei, spätestens nach drei Monaten zu prüfen, ob die Zusammenführung der Daten noch erforderlich ist.

Satz 4 regelt, dass eine Speicherung des Datenbestandes über die in Satz 3 genannte Speicherfrist hinaus nur für 30 Tage erfolgen darf.

Diesbezüglich verpflichtet Satz 5 die Polizei, die nach Satz 4 getroffene Entscheidung zur Aufrechterhaltung der zusammengeführten Daten über die in Satz 3 genannte Speicherfrist hinaus mit Begründung zu dokumentieren.

Aus Verhältnismäßigkeitsgesichtspunkten ordnet Satz 6 an, dass ein Datenbestand, welcher ausschließlich zum Zweck der Erstellung eines Verhaltensprofils zusammengeführt wurde, spätestens nach 30 Tagen zu löschen ist.

Absatz 8

Absatz 8 regelt die Anordnungsbefugnisse entsprechend dem jeweiligen Eingriffsgewicht der Maßnahme.

Satz 1 bestimmt, dass „einfache“ Datenabgleiche nach Absatz 1 (geringes Eingriffsgewicht) zur Suche nach Übereinstimmungen durch jede/n Polizeibedienstete/n angeordnet werden können.

Satz 2 ordnet die Begründungspflicht und die Dokumentationspflicht an.

Satz 3 weist die Anordnungsbefugnis für die automatisierte Datenanalyse mit eingeschränktem Eingriffsgewicht der Behördenleitung zu.

Satz 4 sieht für die Datenanalyse unter Einsatz von selbstlernenden Systemen und zur Erstellung eines Verhaltensprofils die richterliche Anordnung vor.

Satz 5 bestimmt, welche konkreten inhaltlichen Anforderungen an den schriftlichen Antrag zu stellen sind.

Satz 6 regelt, dass die Anordnung zur Erstellung eines Verhaltensprofils immer ausdrücklich erfolgen muss. Dies gilt insbesondere auch, wenn die Anordnung ausschließlich zur Erstellung eines Verhaltensprofils erfolgt.

Satz 7 bestimmt, dass eine Anordnung nach den Absätzen 5 und 6 wegen des Vorliegens von Gefahr in Verzug nur durch den jeweiligen Behördenleiter oder die Behördenleiterin getroffen werden darf.

Im Übrigen regelt Satz 8, dass für die Anordnungen von Maßnahmen nach Absatz 2, 5 und 6 die Anordnungsbestimmungen des § 73 Absatz 2, Absatz 3 Satz 1 und 2 sowie Absatz 4 entsprechend gelten.

Absatz 9

Absatz 9 bestimmt Regelungen, die Vorkehrungen zum Grundrechtsschutz beinhalten.

Satz 1 ordnet an, dass der Zugang zu Anwendungen nach Absatz 2 und 5 auf bestimmte qualifizierte Polizeibedienstete zu beschränken ist und dass Zugriffskontrollen auf die Anwendungen nach Absatz 2 und 5 sicherzustellen sind.

Satz 2 ergänzt die Protokollierungsverpflichtung nach § 75 und ordnet an, dass neben den Protokollierungsinhalten nach § 75 Absatz 1 SächsPVDG auch das zur Datenanalyse eingesetzte System und die Polizeibediensteten, die die jeweilige Maßnahme durchgeführt haben, zu protokollieren sind.

Satz 3 ordnet die Anforderung der Nachvollziehbarkeit des jeweils zur Datenverarbeitung eingesetzten Verfahrens zum Zweck der Gewährleistung von Rechtsschutz und aufsichtlicher Kontrolle sowie der Sicherstellung, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden, an.

Absatz 10

Das Bundesverfassungsgericht gestattet es dem Gesetzgeber, benötigte technisch-organisatorische Regelungen zur Milderung der Eingriffsintensität von Befugnissen bei besonderer Technizität oder rascher Fortentwicklungsmöglichkeit an die Verwaltung zu delegieren.

Mit Absatz 10 wird von der Delegationsmöglichkeit Gebrauch gemacht und das Sächsische Staatsministerium des Innern beauftragt, das Nähere zum Verfahren zu Maßnahmen nach den Absätzen 2 und 5 insbesondere unter Berücksichtigung der gesetzlich angeordneten Regelungsinhalte, in einer Rechtsverordnung zu bestimmen. In den Nummern 1 bis 7 werden die zu regelnden Inhalte benannt.

§ 62b

Mit der neuen Vorschrift des § 62b werden zwei Rechtsgrundlagen für eine nachträgliche Fernidentifizierung eingeführt. Mit Absatz 1 wird eine Befugnis aufgenommen, die den Abgleich von in den polizeilichen Systemen vorhandenen biometrischen Daten mit im Rahmen der konkreten Aufgabenerfüllung erlangten biometrischen Daten bestimmt. In Absatz 2 wird eine Maßnahme eingeführt, die den Abgleich von zur polizeilichen Aufgabenerfüllung gespeicherten biometrischen Daten von Gesichtern und Stimmen mit öffentlich zugänglichen biometrischen Daten aus dem Internet zum Zweck der Identifizierung oder Lokalisierung von Störern bestimmt. Durch eine solche Befugnis können beispielsweise relevante Hinweise zu einer Zielperson, die auf sozialen Netzwerken einen Amoklauf angekündigt hat, gewonnen werden oder der Aufenthaltsort einer Person, von der eine Gefahr für ein überlegend wichtiges Rechtsgut ausgeht, zum Zweck der Abwehr dieser Gefahr ermittelt werden.

Die Befugnis zum Abgleich von gespeicherten biometrischen Daten mit öffentlich zugänglichen biometrischen Daten stellt einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG dar. Durch eine solche Maßnahme erfolgt die Erhebung und Verarbeitung von biometrischen Daten zu einem nicht weiter abgrenzbaren Personenkreis. Gewichtserhöhend wirkt zudem, dass der Abgleich von den betroffenen Personen nicht bemerkt wird, er aus ihrer Sicht also heimlich erfolgt. Bei dieser Ermittlungsbefugnis handelt es sich um eine Maßnahme, die von der Eingriffsintensität heimlichen eingriffsintensiven Überwachungsmaßnahmen gleichkommt. Damit dieser Eingriff in das Grundrecht auf informationelle Selbstbestimmung den Grundsätzen der Verhältnismäßigkeit genügt, gelten als Maßstab für die verfassungsgemäße Ausgestaltung einer gesetzlichen Regelung die Anforderungen des Bundesverfassungsgerichts für die Ausgestaltung von heimlichen Überwachungsmaßnahmen (siehe BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 und 1 BvR 1140/09, Rz. 103 ff, 117ff).

Neben den verfassungsrechtlichen Anforderungen an die Ausgestaltung der Eingriffsschwelle bei intensiven Grundrechtseingriffen hat das Bundesverfassungsgericht weitere Anforderungen aus dem Verhältnismäßigkeitsgrundsatz abgeleitet: Regelungen zur vorherigen Kontrolle, zum Schutz des Kernbereichs, zur Transparenz, zum individuellen Rechtsschutz und zur aufsichtlichen Kontrolle (BVerfG Urteil vom 20. April 2016, Rz. 117ff, 134, 138, 140). Zu diesem Zweck erfolgen Regelungen zum Richtervorbehalt, zu den Anforderungen an die polizeiliche Anordnung (siehe Absatz 6), zum Schutz des Kernbereichs privater Lebensgestaltung (§ 76), zur unverzüglichen Datenlöschung (§ 78), zur Benachrichtigung (§ 74), zur Protokollierung (§ 75), zu den Berichtspflichten (siehe § 107) und zur aufsichtlichen Kontrolle (siehe Absatz 5, § 94, § 2 SächsKontrollG).

Voraussetzung für den Schutz des Kernbereichs privater Lebensgestaltung ist ein Geheimhaltungswillen des Betroffenen. Der vorgesehene Abgleich ist auf öffentlich zugängliche Daten aus dem Internet beschränkt. Diese Daten werden häufig schon deshalb keinen Kernbereichsbezug aufweisen, weil sie von der betroffenen Person selbst öffentlich gemacht wurden, so dass es an dem Geheimhaltungswillen fehlt. Lediglich in Fällen, wenn etwa Bild- oder Tonaufnahmen aus dem Internet in den Abgleich einbezogen werden, die den höchstpersönlichen Lebensbereich einer Person betreffen und ohne den Willen des Betroffenen in das Internet eingestellt wurden, hat die Erhebung von biometrischen Daten Kernbereichsrelevanz. Solange keine Zweifel bestehen, dass die biometrischen Daten ohne oder gegen den Willen des Betroffenen in das Internet hochgeladen wurden, ist der Kernbereichsschutz beim Abgleich nicht tangiert. Nach Hinweisen auf ein widerrechtliches

Hochladen von Bildern, Videos oder Sprachdateien muss die Polizei aktiv suchen; diese können sich bspw. direkt aus dem Inhalt von Videos ergeben oder anhand einschlägig bekannter Internetseiten, auf denen solche Daten gefunden wurden. Bestehen dennoch Zweifel, findet § 76 Absatz 3 und 4 Anwendung.

Absatz 1

Mit Satz 1 wird eine Befugnis zur effizienteren und schnelleren Auswertung von bereits in polizeilichen Systemen vorhandenen Informationen im Zusammenhang mit laufender Sachverhaltsbearbeitung ermöglicht. Die Regelung ermöglicht zum Zweck der Überprüfung der Übereinstimmung den Abgleich von biometrischen Daten, die aus Audio-, Bild- und Video-daten im Rahmen der Aufgabenerfüllung erlangt wurden und solchen biometrischen Daten, die aus weiteren im polizeilichen Datenbestand gespeicherten Daten gewonnen wurden. Es dürfen ausschließlich Daten aus dem Datenbestand der Polizei verarbeitet werden und nur solche, die rechtmäßig erhoben wurden.

Ein besonderer Regelungsbedarf besteht insoweit, als der einfache Datenabgleich nach § 87 SächsPVDG nicht die Verarbeitung biometrischer Daten erlaubt. Auch die allgemeine Datenverarbeitungsklausel des § 54 Absatz 1 Satz 1 SächsPVDG, die zwar die Verarbeitung besonderer Kategorien personenbezogener Daten erlaubt, bildet keine hinreichend spezifische Rechtsgrundlage für den Abgleich von biometrischen Daten.

Der biometrische Abgleich wird nur zur Abwehr einer Gefahr für die öffentliche Sicherheit zugelassen. Damit kann die Maßnahme nicht zum Zweck der Gefahrenforschung erfolgen. Der Sensibilität biometrischer Daten wird mit Satz 2 dadurch Rechnung getragen, dass die Maßnahme zwingend erforderlich sein muss. Dies liegt nur dann vor, wenn die Maßnahme im Einzelfall unverzichtbar ist, um die Gefahren für die öffentliche Sicherheit auszuschließen.

Satz 3 schließt die Verarbeitung personenbezogener Daten aus der Wohnraumüberwachung oder Online-Durchsuchung aus. Daten aus einem Bodycam-Einsatz in Wohnungen sind über § 57 Absatz 8 Satz 6 ausgeschlossen.

Absatz 2

Absatz 2 erlaubt eine anlassbezogene nachträgliche Fernidentifizierung mittels biometrischer Daten, die aus öffentlich zugänglichen Daten aus dem Internet gewonnen wurden. Hierzu zählen nur solche Daten, die von jedermann verwendet werden können, so zum Beispiel Daten aus sozialen Medien. Die Regelung ist auch mit Artikel 5 Absatz 1 Buchstabe e der KI-Verordnung vereinbar, da sie nicht der Verwendung von Systemen dient, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet nutzen, sondern allein die anlassbezogene Erhebung und Verarbeitung von aus dem Internet gewonnenen Daten zum Zweck des biometrischen Abgleichs für die betreffende spezifische Aufgabenerfüllung im Einzelfall erlaubt.

Absatz 2 Satz 1 regelt in den Nummern 1 und 2 zwei unterschiedliche Eingriffsschwellen, die einen Anlass für einen automatisierten biometrischen Datenabgleich bilden können. Die Eingriffsvoraussetzungen sind gegenüber denen des Absatzes 1 deutlicher höher.

Die Eingriffsschwelle in Satz 1 Nummer 1 ist an enge Voraussetzungen geknüpft, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten. Vorausgesetzt wird eine konkrete Gefahr für ein besonders wichtiges Rechtsgut. Satz 1 Nummer 2 erlaubt die Fernidentifizierung biometrischer Daten darüber hinaus in den Fällen, in denen die Identifizierung oder die Ermittlung des Aufenthaltsortes der Person, von der die Gefahr ausgeht, auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Die Eingriffsschwelle in Satz 2 Nummer 1 setzt das Vorliegen einer konkretisierten Gefahr zur Verhütung von besonders schweren Straftaten im Sinne des § 100b Strafprozessordnung voraus. Weiterhin wird eine weitergehende Einschränkung dahingehend getroffen, dass die Straftat auch im Einzelfall besonders schwer wiegen und sich gegen die Rechtsgüter richten muss, die in Satz 1 Nummer 1 genannt werden.

Die Eingriffsschwelle in Satz 2 Nummer 2 regelt das Gefahrenvorfeld und bleibt noch hinter einer konkretisierten Gefahr zurück. Allerdings muss es sich hierbei um die drohende Begehung einer terroristischen Straftat handeln.

Satz 3 bestimmt, dass ein Abgleich der biometrischen Daten, die nach Satz 1 erlangt wurden, nicht mit in Echtzeit übertragenen Video-, Ton- oder Bilddateien erfolgen darf und setzt die Vorgaben des Artikel 5 Absatz 1 UA 1 lit. h KI-VO um.

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

Absatz 3

Absatz 3 stellt klar, wer Adressat der Maßnahmen nach Absatz 1 oder Absatz 2 sein kann. Maßnahmen nach Absatz 2 dürfen zur gezielten Suche nach Störern und zur gezielten Suche nach gefährdeten Personen erfolgen. Maßnahmen nach Absatz 1 dürfen sich nur gegen Störer richten.

Absatz 4

Satz 1 sichert eine strenge Zweckbindung der verarbeiteten biometrischen Daten und der aus dem Internet gewonnenen Daten.

Der Ausschluss der Geltung von § 79a sichert, dass diese Daten weder zu einem anderen Zweck verarbeitet noch zweckkonform genutzt werden dürfen (Satz 2).

Satz 3 ordnet an, dass nicht allein auf der Grundlage des Ergebnisses des Abgleichs polizeiliche Folgemaßnahmen getroffen werden können, sondern erst nach einer Verifizierungsprüfung und begrenzt damit die Beeinträchtigung von Unbeteiligten.

Satz 4 erlaubt die Speicherung des Abgleichsergebnisses und der zur Durchführung des Abgleichs erhobenen Daten erst dann, wenn die Prüfung nach Satz 3 durch Polizeibedienstete dazu geführt hat, dass weitere polizeiliche Maßnahmen erforderlich sind.

Anderenfalls sind nach Satz 5 alle Daten technisch spurlos und automatisiert zu löschen. Somit wird das Entstehen einer Datenbank zur Gesichtserkennung verhindert. Satz 6 sieht eine technische spurlose und automatisierte Löschung ebenfalls für den Fall vor, dass keine Datenübereinstimmung nach Satz 3 vorliegt.

Absatz 5

In Absatz 5 wurde durch die Verweisung auf § 76 Absatz 1 und 5 eine Regelung zum Schutz des Kernbereichs privater Lebensgestaltung aufgenommen.

Absatz 6

Einen Abgleich gemäß Absatz 1 kann jede oder jeder Polizeibedienstete anordnen (Satz 1). Demgegenüber bedürfen Maßnahmen nach Absatz 2 aufgrund des Eingriffsgewichts der richterlichen Anordnung (Satz 2).

Satz 3 trifft darüber hinaus Regelungen über die Form und den Inhalt des Antrags der Polizei.

In Satz 4 wird eine Anordnung wegen des Vorliegens von Gefahr im Verzug unter Behördenleitervorbehalt gestellt.

Absatz 7

Absatz 7 ordnet Regelungen zur Transparenz und Nachvollziehbarkeit dieser grundrechtsintensiven Maßnahmen an. Satz 1 trägt den Anforderungen an grundrechtsintensives Handeln Rechnung, indem nur besonders geschulten Polizeibediensteten der Zugang zu der technischen Anwendung eröffnet wird. Satz 2 ergänzt die Protokollierungspflicht nach § 75 SächsPVDG, indem weitere spezifische Protokollierungspflichten geregelt werden. So ist neben den Polizeibediensteten, die das jeweilige System anwenden, auch die jeweils zum Einsatz gekommene technische Anwendung zu dokumentieren.

Satz 3 ordnet die Anforderung der Nachvollziehbarkeit des jeweils zur Datenverarbeitung eingesetzten Verfahrens zum Zweck der Gewährleistung von Rechtsschutz und aufsichtlicher Kontrolle sowie der Sicherstellung, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden, an.

Durch die in Satz 4 geregelte Verpflichtung, die oder den Sächsische(n) Datenschutz- und Transparenzbeauftragte(n) über abgeschlossene Maßnahmen nach Absatz 2 zu informieren, wird die Möglichkeit einer aufsichtlichen Kontrolle eröffnet und damit die Möglichkeit der Darstellung im jährlichen Bericht gewährleistet.

Satz 5 stellt klar, dass § 94 trotz der Informationspflicht an die oder den Sächsische(n) Datenschutz- und Transparenzbeauftragte(n) unberührt bleibt.

Satz 6 schließt die Anwendung von selbstlernenden KI-Systemen für Maßnahmen nach dieser Vorschrift aus.

Satz 7 bestimmt, dass für Maßnahmen nach Absatz 1 oder 2 auch Hochrisiko-KI-Systeme zur Anwendung kommen können und ordnet für diesen Fall an, dass hierfür die in Artikel 26 der KI-VO genannten Betreiberpflichten durch die Polizei zu erfüllen sind.

Satz 8 setzt weitere Maßgaben der KI-VO um.

Absatz 8

Das Bundesverfassungsgericht gestattet es, dem Gesetzgeber benötigte technisch-organisatorische Regelungen zur Milderung der Eingriffsintensität von Befugnissen bei besonderer Technizität oder rascher Fortentwicklungsmöglichkeit an die Verwaltung zu delegieren. Durch Absatz 8 wird das Sächsische Staatsministerium des Innern durch Verwaltungsvorschrift unter Berücksichtigung der gesetzlichen Maßgaben der Nummern 1 bis 4 verpflichtet, das Nähere zum Verfahren zu regeln. Die Verwaltungsvorschrift ist zu veröffentlichen. Klarstellend wurde eine (bereits nach § 39 Absatz 3 Sächsisches Datenschutz-Umsetzungsgesetz bestehende) Pflicht zur Anhörung der oder des Sächsischen Datenschutz- und Transparenzbeauftragten aufgenommen.

Zu Nummer 18

§ 63

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

Zu Nummer 19

§ 64

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

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

Die Ergänzungen in Absatz 5 dienen der Angleichung an den Einsatz und die Ausschlussgründe zu einer Vertrauensperson durch den Verfassungsschutz und orientieren sich inhaltlich an § 12 Absatz 2 Satz 1, Nr. 3 und 5 sowie Satz 2 SächsVSG, jedoch angepasst an die besonderen Bedürfnisse der Polizeiarbeit.

Die neue Nummer 4 umfasst zwei Fallvarianten von Verbrechen: im ersten Fall kommt es auf den gesetzlichen Strafraum an, nach dem die verübte Straftat mit lebenslanger Freiheitsstrafe bedroht sein muss; daneben können weitere Straftaten (Verbrechen oder Vergehen) in die Verurteilung einbezogen worden sein. Im zweiten Fall kommt es auf die Höhe der tatsächlich durch das Gericht verhängten Freiheitsstrafe für eine Straftat (allein) an. Auch hier kann in die Verurteilung weitere Straftaten einbezogen worden sein. In beiden Fällen wird auf die Schwere eines verurteilten Verbrechens abgestellt.

Sofern ein Einsatz einer bestimmten V-Person untersagt ist, hat bereits ihre Anwerbung zu unterbleiben.

Zu Nummer 20

§ 65

Mit der Änderung der Verweisung erfolgt eine redaktionelle Folgeanpassung.

Zu Nummer 21

§ 66

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

Absatz 1

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

Absatz 2

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

in der Hard- oder Software maßgeschneidert. Gleichwohl ist sie ein unverzichtbares Instrument einer erfolgreichen Gefahrenaufklärung im Bereich von terroristischen Gefährdern oder Organisierter Kriminalität.

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

Absatz 2a

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

Nummer 1 setzt für die Quellen-TKÜ das Vorliegen einer gegenwärtigen Gefahr (siehe Begriffsbestimmung in § 4 Nummer 3b) für die in der Regelung explizit benannten Rechtsgüter voraus. Der Sachwertgüterschutz wird beschränkt auf die Gefährdung von Gütern der Allgemeinheit, deren Bedrohung die Existenz der Menschen berührt. Dies können wesentliche Infrastruktureinrichtungen sein (z. B. Kraftwerke, Wasserwerke) oder Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen (Hochspannungsmasten). Im Unterschied zum Sachwertgüterschutz nach Absatz 1 unterfallen Kulturgüter, deren Erhaltung im öffentlichen Interesse geboten ist, nicht dem Sachwertschutz nach Absatz 2a.

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

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

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

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

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

Absatz 3

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

Absatz 4

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

Absatz 5

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

Absatz 6

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

§ 66a

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

Absatz 1

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

Absatz 2 bis 5

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

Absatz 6

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

§ 67

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

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

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

§ 68

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

Absatz 1

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

Absatz 2

In Absatz 2 wurde die Regelung des bisherigen § 71 Absatz 1 überführt und die Eingriffsschwellen dahingehend modifiziert, dass die bisherige Anforderung, dass die Ermittlung des Aufenthaltsortes auf andere Weise „aussichtslos oder wesentlich erschwert wäre“ auf „weniger Erfolg versprechend oder erschwert wäre“, herabgesetzt wurde. Weiterhin wurde in Absatz 2 ein Verweis auf die einschlägigen Vorschriften zur Definition des „Anbieters von Telekommunikationsdiensten“ im Telekommunikationsgesetz und zur Definition des „Anbieters von digitalen Diensten“ im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz aufgenommen. Der Verweis dient der Klarstellung hinsichtlich des Kreises der zur Herausgabe der Daten Verpflichteten.

Absatz 3

In Satz 1 wurde die Regelung des bisherigen § 68 Absatz 2 Satz 1 und des § 71 Absatz 3 Satz 1 überführt. Satz 2 und 3 beinhalten jeweils die Regelung des bisherigen § 68 Absatz 2 Satz 2 und des bisherigen § 71 Absatz 3 Satz 2 zur Zweckbindung. Satz 4 überführt die Regelungen aus § 68 Absatz 2 Satz 3 und § 71 Absatz 3 Satz 3.

Absatz 4

Satz 1 beinhaltet die Regelung des bisherigen Absatzes 3 mit einer redaktionellen Anpassung. Satz 2 beinhaltet die Regelung des bisherigen § 71 Absatz 4. In Satz 4 erfolgte eine sprachliche Klarstellung.

Zu Nummer 22

§ 69 (gestrichen)

Der bisherige Regelungsinhalt wurde in § 66a überführt.

Zu Nummer 23

§ 70

Zielsetzung der Änderungen ist die Umsetzung des Beschlusses des Bundesverfassungsgerichts vom 27. Mai 2020 (1 BvR 1873/13, - 1 BvR 2618/13 – „Bestandsdatenauskunft II“). Das Bundesverfassungsgericht hatte mit diesem Beschluss § 113 des Telekommunikationsgesetzes und mehrere Fachgesetze des Bundes, die die manuelle Bestandsdatenauskunft regeln, für verfassungswidrig erklärt. Die Erteilung von solchen Auskünften sei grundsätzlich verfassungsrechtlich zulässig, jedoch müssten Übermittlungs- und Abrufregelungen durch hinreichend begrenzte Eingriffsschwellen die Verwendungszwecke beschränken. Das Gericht hat seine Anforderungen an die Ausgestaltung des „Doppeltürmodells“ weiter konkretisiert. Für allgemeine Bestandsdaten sei das Vorliegen einer konkreten Gefahr im Einzelfall ausreichend (BVerfG a. a. O, Rz. 146). Soweit eine Zuordnung von Bestandsdaten über Internetprotokolladressen erfolge, müsse dem erhöhten Eingriffsgewicht durch den Schutz von Rechtsgütern von zumindest hervorgehobenen Gewicht Rechnung getragen werden (BVerfG, a. a. O, Rz. 177). Über Zugangsdaten dürfe nur dann Auskunft erteilt werden, wenn die gesetzlichen Voraussetzungen für ihre Nutzung vorliegen (BVerfG, a. a. O, Rz. 235). Ferner bedurfte es der Anpassung an bundesgesetzliche Änderungen. Die jeweiligen Anforderungen müssten bereits in den Übermittlungsregelungen („1. Tür“) vollständig bestimmt sein und könnten nicht erst in den fachgesetzlichen Abrufregelungen („2. Tür“) geregelt werden (BVerfG, a. a. O, Rz. 134).

Absatz 1

Satz 1 beinhaltet wie bisher die Eingriffsschwelle für die einfache Bestandsdatenauskunft. Die Regelung setzt die Vorgaben des Bundesverfassungsgerichts um, da Voraussetzung

für den Abruf von (einfachen) Bestandsdaten das Vorliegen einer konkreten Gefahr für die öffentliche Sicherheit im Einzelfall ist. Bei den Anpassungen handelt es sich um redaktionelle Anpassungen im Hinblick auf Änderungen in den Bundesgesetzen. Die bisherigen Regelungsinhalte der §§ 95, 111 Telekommunikationsgesetz finden sich jetzt in §§ 3 Nummer 6, 174 Telekommunikationsgesetz, die damaligen Regelungsinhalte des § 14 Telemediengesetzes in § 2 Absatz 2 Nummer 2 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz.

Satz 2 beinhaltet wie bisher die Eingriffsschwelle für Auskünfte über Zugangsdaten nach dem Telekommunikationsgesetz (Nummer 1) und nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (Nummer 2). Das Bundesverfassungsgericht hat hier wiederholend festgestellt, dass im Anwendungsbereich des Telekommunikationsgesetzes diese Auskünfte nur erteilt werden dürfen, wenn die gesetzlichen Voraussetzungen für die Nutzung vorliegen. Dem trägt die bestehende Regelung bereits Rechnung. Bei der Anpassung handelt es sich um eine redaktionelle Anpassung im Hinblick auf Änderungen im Telekommunikationsgesetz. Satz 2 Nummer 2 enthält die Befugnis für die Erlangung von Zugangsdaten im Hinblick auf digitale Dienste. Mit der Benennung der Rechtsgüter Leib, Leben oder Freiheit der Person, sexuelle Selbstbestimmung, Bestand des Bundes oder eines Landes oder Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, wird die Übereinstimmung mit der bundesrechtlichen Eingriffsschwelle der Übermittlungsvorschrift im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (§ 23 Absatz 2 Nummer 2 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz) gewährleistet.

Absatz 2

Die Regelung beinhaltet wie bisher die Eingriffsschwelle, wenn Ausgangspunkt der polizeilichen Anfrage auf Auskunft über einfache Bestandsdaten eine Internet-Protokoll-Adresse ist. Die bisherige Regelung genügte nicht den Anforderungen des Bundesverfassungsgerichts. Um den Anforderungen zu genügen, wurde die Auskunft dahingehend eingegrenzt, dass diese dem Schutz von Rechtsgütern von hervorgehobenem Gewicht dienen muss. Dementsprechend werden in der Regelung die Rechtsgüter Bestand oder Sicherheit des Bundes oder eines Landes, Leib, Leben oder Freiheit einer Person oder für Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt oder deren Erhaltung im öffentlichen Interesse geboten ist, aufgenommen. Die Eingriffsschwelle stimmt mit den bundesrechtlichen Eingriffsschwellen der Übermittlungsvorschriften im Telekommunikationsgesetz bzw. im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz überein.

Absatz 3

Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichts (BVerfG, a. a. O., Rz. 252), dass die Bestandsdatenauskunft auf der Grundlage der Internet-Protokolladresse keiner richterlichen Anordnung bedürfe, erfolgt die Streichung des Verweises auf Absatz 2.

Absatz 4

Satz 1 beinhaltet die Regelung des bisherigen § 72 Absatz 2 Nummer 3 mit redaktionellen Anpassungen. Satz 2 beinhaltet die Regelung des bisherigen § 72 Absatz 4.

§ 71

Aus rechtssystematischen Gründen wurde der bisherige Regelungsinhalt des § 71 in die Vorschrift § 68 übernommen. In die Vorschrift wurde im Regelungszusammenhang zu den eingriffsintensiven Befugnissen eine Rechtsgrundlage für den Einsatz von unbemannten Luftfahrtsystemen aus Gründen der Klarstellung der Zulässigkeit der Drohnenverwendung für bestimmte Datenerhebungsmaßnahmen aufgenommen.

Absatz 1

Satz 1 regelt, bei welchen Datenerhebungsmaßnahmen unter den Voraussetzungen der jeweils genannten Befugnisregelungen ein Drohneneinsatz zur Datenerhebung zulässig sein kann. Mit der Regelung erfolgt keine Befugnisserweiterung. Satz 2 stellt klar, dass offene Bildbeobachtungen nach § 57 Absatz 1 und offene Bild- und Tonaufzeichnungen nach § 56, § 57 Absätze 2 und 3 auch im Fall eines Drohneneinsatzes den Charakter als offene Maßnahme bewahren müssen. Satz 3 verpflichtet, durch geeignete Maßnahmen (z.B. besondere Kennzeichnung des polizeilichen „Drohnepilots“ oder Hinweis bei der jeweiligen Veranstaltung), auf die Verwendung der Drohne aufmerksam zu machen.

Absatz 2

Absatz 2 ähnelt Absatz 1 Satz 1 Nummer 2 und ermöglicht offene Bildübertragungen im öffentlichen Verkehrsraum zum Zweck der Lageübersicht in zwei Fallkonstellationen; einmal zur Lenkung und Leitung von Verkehrsmaßnahmen sowie zum anderen bei Unglücks- und Verkehrsunfällen. Eine Datenaufzeichnung und eine Personenidentifizierung sind dabei ausdrücklich ausgeschlossen. Auch hier ist, wie zu allen offenen Maßnahmen, in geeigneter Weise auf die Datenerhebung durch Drohnenüberflüge hinzuweisen.

Absatz 3

Die Regelung stellt in Satz 1 klar, dass soweit richterliche Anordnungen für Maßnahmen nach Absatz 1 erforderlich sind, diese auch den Einsatz von unbemannten Luftfahrtsystemen umfassen müssen. Die Regelung in Satz 2 dient der Klarstellung, dass Drohnen nicht genutzt werden dürfen für den Einsatz von Waffen.

Zu Nummer 24

§ 72

Aus rechtssystematischen Gründen und aus Gründen der Anwenderfreundlichkeit wurde der Regelungsinhalt des bisherigen § 72 jeweils in die Vorschriften § 66 Absatz 5, § 66a Absatz 7, § 67 Absatz 3 und § 70 Absatz 4 überführt. Die Vorschrift ist daher zu streichen.

Zu Nummer 25

§ 73

Die Inhalte der bisherigen Regelung des § 73 wurden aus Gründen der Klarstellung in nunmehr fünf Absätze gegliedert.

Absatz 1

Absatz 1 bestimmt, dass für nach dem Sächsischen Polizeivollzugsdienstgesetz geregelte gerichtliche Entscheidungen die Maßgaben der nachfolgenden Absätze 2 bis 5 gelten.

Absatz 2

Absatz 2 beinhaltet die bisherige Regelung des § 73 Absatz 1 Nummer 1.

Absatz 3

Satz 1 beinhaltet die bisherige Regelung des § 73 Absatz 1 Nummer 2 Satz 1 mit Änderungen. Die Ergänzungen erfolgen in Konsequenz der Aufnahme neuer Befugnisregelungen. Satz 2 beinhaltet die bisherige Regelung des § 73 Absatz 1 Nummer 2 Satz 2. Satz 3 beinhaltet die bisherige Regelung des § 73 Absatz 1 Nummer 2 Satz 3. Satz 4 enthält zur Klarstellung die Verweisungen auf spezifische Fristenregelungen, die der Regelung in Satz 3 vorgehen.

Absatz 4

Satz 1 beinhaltet die bisherige Regelung des § 73 Absatz 2 Satz 1. Satz 2 beinhaltet die bisherige Regelung des § 73 Absatz 2 Satz 2. Satz 3 wurde im Hinblick auf Maßnahmen nach § 57a in Umsetzung der Regelung des Artikels 5 Absatz 3 KI-VO eingefügt, im Hinblick auf Maßnahmen nach § 62a Absatz 5 und § 62b Absatz 2 erfolgt eine von Satz 3 abweichende Regelung aus Gründen der Eingriffsintensität der Befugnis. In Satz 4 und 5 wird die gesetzliche Löschanordnung, anknüpfend an die unterschiedlichen richterlichen Bestätigungsfristen (24 Stunden, 48 Stunden), ergänzend geregelt.

Absatz 5

Die Regelung beinhaltet die bisherige Regelung des § 73 Absatz 3. Im Hinblick auf die neue Befugnis in § 57a bestand Ergänzungsbedarf.

§ 74

Absatz 1

Die Änderungen oder Ergänzungen in Satz 1 erfolgen in Konsequenz der Aufnahme neuer benachrichtigungspflichtiger Befugnisse (§ 57a, § 62b) in das Sächsische Polizeivollzugsdienstgesetz, der Streichung der bisherigen Befugnis in § 59 oder sie stellen redaktionelle Folgeänderungen dar.

In Nummer 1 wurde eine Benachrichtigungspflicht im Hinblick auf die neue Befugnis zur Datenverarbeitung nach § 57a Absatz 1 Satz 4 und Absatz 2 im Hinblick auf die Zielperson der jeweiligen Maßnahme aufgenommen.

Nummer 2 dient der Klarstellung, dass eine Benachrichtigungspflicht bei Maßnahmen nach § 58 nur dann besteht, soweit im Ergebnis der manuellen Verifizierung eines Trefferfalls ein Echttreffer vorliegt. Nur in diesem Fall, in dem eine Weiterverarbeitung der personenbezogenen Daten erfolgt, ist eine Benachrichtigung der betroffenen Person zur Gewährleistung von Rechtsschutz zweckmäßig.

Die Ergänzung in Nummer 3 erfolgt in Konsequenz der Ergänzung des § 60 um den Ausschreibungsgrund der Erkenntnisanfrage.

Die Änderung in Nummer 5 erfolgt vor dem Hintergrund, dass es sich bei der automatisierten Datenanalyse nach § 62a Absatz 2, 5 und 6 um eine eingriffsintensive Maßnahme handelt. Eine Benachrichtigungspflicht besteht in diesem Fall jedoch nur dann gegenüber einer Person, wenn durch die automatisierte Datenanalyse neue Erkenntnisse erlangt wurden. Darüber hinaus besteht eine Benachrichtigungspflicht der betroffenen Person, wenn über diese ein Verhaltensprofil gemäß § 62a Absatz 6 erstellt wurde.

Die Änderung in Nummer 6 erfolgt in Konsequenz der Aufnahme der neuen Befugnis in § 62b Absatz 2 zur nachträglichen Fernidentifizierung.

Die Änderungen in den Nummern 1 bis 14 sind Folge der systematischen Änderungen der Befugnisregelungen in den §§ 66a bis 68.

Die Änderung in Nummer 15 ist redaktionell. Die Benachrichtigungspflicht in Bezug auf Maßnahmen nach § 70 war bisher in Nummer 13 geregelt. Weiterhin bestand das Erfordernis der Umsetzung des Artikels 26 Absatz 11 der KI-VO. Danach ist die betroffene Person, soweit der Einsatz eines Hochrisiko-KI-Systems erfolgt, auch darüber zu informieren, dass die zu ihrer Person verarbeiteten Daten durch den Einsatz eines solchen Hochrisiko-KI-Systems erfolgt sind.

Absatz 2

Die Änderungen in Satz 1 sind Konsequenz redaktioneller Änderungen in Absatz 1 Satz 1.

Absatz 3

Mit der Änderung in Satz 3 wird eine klarstellende Regelung aufgenommen, dass die Strafverfolgungsbehörden nicht nur über das „ob“ der Zurückstellung, sondern auch über die Fristen der Benachrichtigung entscheiden. Mit der Änderung wird einer Regulationsbitte des Sächsischen Staatsministeriums der Justiz nachgekommen.

§ 75

Die Änderungen oder Ergänzungen in Absatz 1 und Absatz 2 erfolgen in Konsequenz der Aufnahme neuer benachrichtigungspflichtiger Befugnisse (§ 57a, § 62a, § 62b) in das Sächsische Polizeivollzugsdienstgesetz, der Streichung der bisherigen Befugnis in § 59 oder sie stellen redaktionelle Folgeänderungen dar.

Zu Nummer 26

§ 76

Die Änderung in Absatz 2 Satz 3 stellt eine redaktionelle Folgeanpassung an Änderungen des § 61 dar.

Zu Nummer 27

§ 78

Die Ergänzungen und Änderungen stellen jeweils Folgeanpassungen dar.

Zu Nummer 28

§§ 79 bis 80d

Vorbemerkung zu den Änderungen und Ergänzungen in den §§ 79 bis 80d

Aus rechtssystematischen Gründen, zur Verbesserung der Anwenderfreundlichkeit und insbesondere zur Umsetzung der Rechtsprechung des Bundesverfassungsgerichts sowie des Sächsischen Verfassungsgerichtshofs wurde die Regelungssystematik der Vorschriften zur Datenverarbeitung umgestaltet und umfassend geregelt. Aus Gründen der Anwenderfreundlichkeit wurden ergänzend Datenverarbeitungsbefugnisse aufgenommen, um die Zulässigkeit der Datenverarbeitung in den erforderlichen logischen Zusammenhängen umfassend zu regeln und das Erfordernis ergänzender Anwendung allgemeiner datenschutzrechtlicher Vorschriften (Sächsisches Datenschutz-Umsetzungsgesetz) auszuschließen. Zudem bestand in Folge des Urteils des Bundesverfassungsgerichts vom 1. Oktober 2024, 1 BvR 1160/19, Bundeskriminalamtgesetz II, Bedarf für eine gesetzgeberische Gestaltung der Anforderungen an eine Datenbevorratung (Herkunft, Art, Umfang), zu den zulässigen Speicherfristen von für auf Vorrat gespeicherte Daten zu bestimmen und schließlich die Anforderungen zu regeln, wenn bevorratete Daten genutzt.

Vor diesem Hintergrund wurden:

- in dem geänderten § 79 zunächst die (allgemeinen) Befugnisse zur Datenverarbeitung zu den bestehenden zulässigen Zwecken geregelt, die da sind: polizeiliche Aufgabenerfüllung, Vorgangsverwaltung und befristete Dokumentation zusammenfassend geregelt,

- in § 79a neu (bisher § 79) sodann die Befugnisse (Voraussetzungen und Grenzen) zur Datenweiterverarbeitung im Rahmen der Zweckbindung und im Rahmen der Zweckänderung bestimmt,
- in § 79b neu (bisher § 80) folgen sodann die besonderen Befugnisregelungen zur Zulässigkeit spezifischer Datenweiterverarbeitungszwecke aufgenommen, als da sind: die Aus- und Fortbildung, die wissenschaftliche Forschung, die Prävention von Straftaten oder die zweckändernde Verarbeitung von Vorgangsdaten zur Abwehr von Gefahren für hochrangige Rechtsgüter,
- in § 79c aus rechtssystematischen Aspekten die neue Befugnis zur Weiterverarbeitung vorhandener Daten zu Zwecken des Trainings und den Test von lernenden IT-Systemen als besonderer Zweckänderungsvorschrift aufgenommen,
- in den §§ 80, 80a, 80b und § 80c in Umsetzung des Urteils des Bundesverfassungsgerichts zur Zulässigkeit der Datenbevorratung vom 1. Oktober 2024, 1 BVR 1160/19, unterschieden nach den Kategorien von Personen (§ 28 SächsDSUG) und der Herkunft der Daten, Regelungen zu den Voraussetzungen vorsorgende Speicherungen und im Hinblick auf das Urteil des Sächsischen Verfassungsgerichts vom 25. Januar 2024 (Vf. 91-II-19) die Anforderungen, wenn bevorratete Daten genutzt werden, klar bestimmt,
- in § 80d schließlich der gesetzliche Rahmen für die Aussonderungsprüffristen unterschieden danach, ob die Speicherung von Daten für die konkrete Aufgabenbestimmung erfolgt oder ob die Speicherung vorsorgend erfolgt, normiert.

Aus Gründen der Klarstellung wurden die Regelung des § 91 Absatz 3 im Hinblick auf sämtliche Tatbestände, die zur Löschung von personenbezogenen Daten führen, klarstellend ergänzend erweitert.

§ 79

Absatz 1

Mit Absatz 1 wird im Sächsischen Polizeivollzugsdienstgesetz nunmehr eine allgemeine Datenverarbeitungsbefugnis aufgenommen, die es der Polizei erlaubt, personenbezogene Daten zur Aufgabenerfüllung in Dateisystemen zu verarbeiten, soweit dies erforderlich ist. Der Begriff des „Verarbeitens“ bildet den Oberbegriff (siehe Begriffsbestimmung „Verarbeiten“ in § 2 Nummer 3 SächsDSUG) für verschiedene Arten der Datenverarbeitung. Er erfasst insbesondere die Speicherung personenbezogener Daten. Da eine solche allgemeine Datenverarbeitungsbefugnisregelung im Sächsischen Polizeivollzugsdienstgesetz bisher fehlte, war im Hinblick auf die Befugnis zur Speicherung von Daten zur Aufgabenerfüllung immer ein „Rückgriff“ auf die allgemeine Vorschrift des § 3 Absatz 1 SächsDSUG erforderlich. Mit der Aufnahme der Regelung in das Sächsische Polizeivollzugsdienstgesetz wird diese bereichsspezifische Regelungslücke nunmehr geschlossen und die Anwenderfreundlichkeit erhöht.

Absatz 2

Absatz 2 beinhaltet die bisher in § 80 Absatz 7 enthaltene Befugnis zur Verarbeitung personenbezogener Daten zu Zwecken der Vorgangsverwaltung oder zu Zwecken der befristeten Dokumentation mit der bestehenden engen Zweckbindung.

Absatz 3

Die Regelung in Absatz 3 stellt klar, dass, soweit gesetzliche Regelungen die Einrichtung von Informationsverbünden unter Beteiligung der Polizei vorsehen (Beispiel hierfür ist § 29

BKAG), für die Datenverarbeitung durch die Polizei Sachsen in dem betreffenden Dateisystem des Informationsverbundes, unbeachtet sonstiger gesetzlicher Anforderungen an die Datenverarbeitung in dem Informationsverbund (Beispiel ist § 30 BKAG), für die Zulässigkeit der Datenverarbeitung durch die Polizei Sachsen die Regelungen des Sächsischen Polizeivollzugsdienstgesetzes maßgeblich sind.

Absatz 4

Mit der Regelung wird eine bestehende Befugnislücke, angelehnt an die Regelung in § 16 Absatz 6 BKAG, geschlossen (siehe auch § 34 Absatz 6 PolDVG HH, § 71 Absatz 2 PolG BW). Zum Schutz einer Person oder zur Eigensicherung von Polizeibediensteten kann die Speicherung von personengebundenen Hinweisen (PHW) erforderlich sein. Beispiele für PHW sind „bewaffnet“, „gewalttätig“, „Freitodgefahr“. Die Vergabe eines PHW erfolgt im Einzelfall und umfasst jeweils die Prüfung der Erforderlichkeit, Geeignetheit und der Verhältnismäßigkeit im engeren Sinne. Am Beispiel des PHW „Freitodgefahr“ kann die Polizei bei Bedarf (beispielsweise im Hinblick auf Festnahme oder Ingewahrsamnahme) bereits im Vorfeld geeignete Maßnahmen ergreifen, um die Suizidgefahr des Betroffenen abzuwehren. Vorhandene Erkenntnisse über Aggressionen gegen Polizeibedienstete vor dem Hintergrund religiöser oder weltanschaulicher Überzeugungen können die Speicherung des PHW „gewalttätig“ rechtfertigen. Die Regelung lässt darüber hinaus die Verarbeitung von ermittlungsunterstützenden Hinweisen (EHW) zu, wenn sie geeignet sind, dem Schutz Dritter oder der Gewinnung von weiteren Ermittlungshinweisen zu dienen. Ermittlungsunterstützende Hinweise sind Hinweise auf Besonderheiten einer natürlichen Person, die dazu geeignet sind, einen polizeilichen Kontext zu verdeutlichen, polizeiliches Handeln zielgerichteter zu steuern bzw. zu unterstützen oder die dem Schutz Dritter dienen. Beispiele für EHW sind „Kfz-Dieb“, „Reisender Täter“, „Intensivtäter“. Es ist zu beachten, dass PHW und EHW nur vergeben werden können, soweit zu der jeweiligen Person ein speicherfähiger Bezugssachverhalt vorliegt. Über die bundeseinheitlich abgestimmten Leitfäden zur Vergabe von PHW und EHW wird die Vergabe vereinheitlicht.

§ 79a

Absatz 1

Zur Klarstellung, dass sich Satz 1 (in Abgrenzung zu Satz 2) auf Daten bezieht, die die Polizei selbst erhoben hat, erfolgt die Aufnahme des Wortes „selbst“. Mit der Ergänzung „unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift“ werden die Anforderungen an den Prüfungsmaßstab einer weiteren Nutzung von Daten über den konkreten Anlass hinaus im Rahmen des ursprünglichen Zwecks (zweckwahrende Nutzung) nach Maßgabe der Ausführungen des BVerfG präzisiert (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rz. 278 ff).

Satz 2 entspricht der bisherigen Regelung in § 79 Absatz 1 Satz 2.

Absatz 2

Die Ergänzung in Satz 2, dass Vorschriften dieses Gesetzes und andere Rechtsvorschriften zur zweckändernden Weiterverarbeitung unberührt bleiben, stellt klar, dass spezifisch geregelte Weiterverarbeitungsbefugnisse, die eine zweckändernde Verarbeitung von personenbezogenen Daten erlauben, die Regelung des Satzes 1 verdrängen. Beispiel hierfür sind die Regelungen in Absatz 4, § 79b und die §§ 80 ff.

Absatz 3

Mit der Regelung wird eine Rechtsgrundlage für die zweckändernde Verarbeitung von Daten aus der polizeilichen Aufgabenerfüllung zu Zwecken der Gefahrenvorsorge (Prävention) aufgenommen. Die Regelung ermöglicht die Weiterverarbeitung von Adressdaten von Mit-

gliedern der extremistischen Szene, zu denen Erkenntnisse zur Begehung politisch motivierter Straftaten vorliegen, zum Zweck der Täteransprache und der Beratung durch die Polizei im Rahmen des Aussteigerprogramms Sachsen.

Absatz 4

Die Regelung des Absatzes 4 entspricht dem bisherigen § 79 Absatz 3.

Absatz 5

Absatz 5 entspricht der Regelung des bisherigen § 79 Absatz 4.

Absatz 6

Absatz 6 entspricht der bisherigen Regelung des § 79 Absatz 5.

§ 79b

In der Vorschrift werden die bisherigen Befugnisregelungen zur Weiterverarbeitung von zu Zwecken der Aufgabenerfüllung erhobenen personenbezogenen Daten zu Zwecken der Aus- und Fortbildung, zu statistischen Zwecken und wissenschaftlichen Zwecken zusammengefasst. Weiterhin geregelt wird die Zulässigkeit der Weiterverarbeitung von zu Zwecken der Vorgangsverwaltung, der zeitlich befristeten Dokumentation polizeilichen Handelns oder von zu Zwecken der Protokollierung gespeicherten Daten. Die Weiterarbeitung zu archivarischen Zwecken entfällt aufgrund des Umstands, dass sich die Weiterverarbeitung zu derartigen Zwecken nach den Regelungen des Sächsischen Archivgesetzes richtet.

Absatz 1

Die Regelung entspricht der Bisherigen in § 80 Absatz 6.

Absatz 2

Mit der Aufnahme einer spezifischen Befugnis zur Weiterverarbeitung von personenbezogenen Daten aus der polizeilichen Aufgabenerfüllung zu wissenschaftlichen Zwecken wird aus rechtssystematischen Gründen entsprechend der Regelung in § 6 Sächsisches Datenschutz-Umsetzungsgesetz eine bereichsspezifische Regelung getroffen.

Absatz 3

Die Regelung in Absatz 3 Satz 1 erlaubt unter Beachtung der Grundsätze des § 79a Absatz 2 eine zweckändernde Verarbeitung von personenbezogenen Daten, die ursprünglich zu Zwecken der Vorgangsverwaltung oder zur zeitlich befristeten Dokumentation behördlichen Handelns gespeichert worden sind. Durch ein redaktionelles Versehen wurde die Regelung jedoch im Rahmen der Novelle des Polizeirechts in 2019 nicht in das Sächsische Polizeivollzugsdienstgesetz überführt. Die Ergänzung dient der Korrektur. Zur Weiterverarbeitung von Protokolldaten, die originär nicht zur polizeilichen Aufgabenerfüllung, sondern vielmehr aufgrund einer allgemeinen datenschutzrechtlichen Verpflichtung erhoben und verarbeitet werden, verweist Satz 2 auf die Regelung des § 32 Absatz 1 Sächsisches Datenschutz-Umsetzungsgesetz.

§ 79c

In § 79c wurde analog zu der Regelung in § 37a PolDVG HH eine Befugnis aufgenommen, vorhandene personenbezogene Daten der Polizei zum Zweck des Entwickelns, des Trainierens und Testens von IT-Systemen weiterverarbeiten zu dürfen. Vor dem Hintergrund der neuen Befugnisregelungen in den §§ 57a Absatz 1 Satz 1, 3 und 4 sowie Absatz 2, 62a und 62b, die den Einsatz KI gestützter technischer Systeme erfordern, besteht Bedarf zum

Zweck des Entwickelns, des Trainings oder Testens entsprechender Software. Ziel ist es, durch Training mit polizeilichen Daten nachvollziehbare Datenverarbeitungsschritte in der jeweiligen (eigen- oder fremdentwickelten) Software zu programmieren und damit die jeweilige spezifische Datenverarbeitung, so beispielsweise die Mustererkennung nach § 57a Absatz 1 Satz 1 oder die biometrische Echtzeit-Identitätsfeststellung gemäß § 57a Absatz 1 Satz 4 oder Absatz 2 in besonderen Gefahrensituationen durch regelbasierte, austrainierte und ausgelernete Systeme zu ermöglichen. Entsprechendes gilt für § 62a Absatz 5 SächsPVDG, der den Einsatz von selbstlernenden Systemen ermöglicht.

Absatz 1

Satz 1 erlaubt der Polizei zum Zweck des Entwickelns, des Trainierens oder Testens von IT-Systemen, rechtmäßig gespeicherte personenbezogene Daten weiterzuverarbeiten. Die Regelung knüpft an das Erfordernis der Weiterverarbeitung der Daten für die Aufgabenerfüllung an. Sie erlaubt, dass Daten zu dem Zweck auch an Dritte oder Auftragsdatenverarbeiter übermittelt werden dürfen. Weiterhin wird klargestellt, dass eine solche Verarbeitung personenbezogener Daten im Hinblick auf das jeweils vorgesehene IT-System nur erfolgen darf, wenn der Einsatz des betreffenden IT-Systems auch für die Aufgabenerfüllung erforderlich ist.

Satz 2 enthält eine weitere Einschränkung dahingehend, dass die Einbeziehung von personenbezogenen Daten bei dem Training von IT-Systemen auf solche zu beschränkt ist, die im Zusammenhang mit der zu trainierenden Aufgabe verarbeitet worden sind.

Satz 3 dient der Verhinderung der Herausbildung von diskriminierenden Algorithmen und ergänzt insoweit den Regelungsinhalt von Satz 5.

Satz 4 setzt das Verbot der Verwendung von Systemen zur biometrischen Kategorisierung, mit denen natürliche Personen auf der Grundlage ihrer biometrischen Daten kategorisiert werden, nach Artikel 5 Absatz 1 Unterabsatz 1 lit. g KI-VO um.

Satz 5 beinhaltet die gesetzliche Anordnung durch technische und organisatorische Maßnahmen die Nachvollziehbarkeit der Datenverarbeitungsschritte des betreffenden Verfahrens sicherzustellen.

Mit Satz 6 wird durch die Verpflichtung zur Dokumentation die Nachvollziehbarkeit der Verarbeitung der verwendeten Daten sichergestellt.

Satz 7 schließt aus Gründen der Verhältnismäßigkeit die Weiterverarbeitung von personenbezogenen Daten zu Zwecken nach Satz 1 (auch durch Übermitteln an Dritte oder Auftragsverarbeiter) aus Maßnahmen nach §§ 65, 66 SächsPVDG oder erlangter Daten aus einer Online-Durchsuchung, § 79a Absatz 4 Satz 3 SächsPVDG, aus. Weitere strikte Zweckbindungsregelungen, u. a. in den §§ 57, 57a, 62b SächsPVDG, schließen eine Weiterverarbeitung von aus diesen Befugnissen erlangten personenbezogenen Daten zu Zwecken nach § 79c Absatz 1 darüber hinaus aus.

Absatz 2

Satz 1 verpflichtet die Polizei aus Gründen der Verhältnismäßigkeit zum Zweck des Entwickelns, Trainierens oder Testens vorrangig anonymisierte Daten zu verwenden und bestimmt die Voraussetzungen für Ausnahmen von der Verpflichtung zur Verwendung anonymisierter Daten. Satz 3 stellt klar, dass besondere Kategorien von personenbezogenen Daten nur gemäß § 4 Absatz 2 SächsDSUG verarbeitet werden dürfen. Satz 4 ordnet eine Lösungsverpflichtung, soweit personenbezogene Daten nicht mehr erforderlich sind für die Zwecke der Entwicklung, Trainierens oder Testens. Satz 5 sichert die erforderliche Löschung durch die Verpflichtung zur Protokollierung. Satz 6 beinhaltet ein Wiederherstellungsverbot von zu löschenden personenbezogenen Daten und ein Verbot der Deanonymisierung.

Absatz 3

Die Sätze 1 und 2 bestimmen, unter welchen Voraussetzungen vorhandene personenbezogene Daten der Polizei an Dritte oder Auftragsdatenverarbeiter zum Zweck der Entwicklung, des Testens und Trainierens von für die Aufgabenerfüllung der Polizei erforderliche IT-Systeme übermittelt werden dürfen.

Absatz 4

Die Sätze 1 und 2 enthalten besondere Maßgaben zur Verhinderung von im Zusammenhang mit der Übermittlung von polizeilichen Daten an Dritte oder Auftragsdatenverarbeiter bestehenden Gefahren des Datenmissbrauchs. Satz 3 verpflichtet zu technisch-organisatorischen Maßnahmen, die die Einhaltung der Maßgaben der Sätze 1 und 2 sicherstellen.

Absatz 5

Adressat der Regelungen in den Sätzen 1 und 2 sind die Dritt- oder Auftragsdatenverarbeiter. Durch die Regelungen werden diese grundsätzlich verpflichtet, erlangte Daten nach Abschluss des Trainings und des Tests zu löschen. Die Zulässigkeit einer Weiternutzung wird unter einen ausdrücklichen Genehmigungsvorbehalt der Polizei gestellt.

Absatz 6

Absatz 6 verpflichtet das Sächsische Staatsministerium des Innern, das Nähere zu dem Verfahren des Testens oder Trainierens von lernenden KI-Systemen durch Verwaltungsvorschrift nach Maßgabe der Anforderungen der Nummern 1 bis 8 zu regeln. Klarstellend wurde die Verpflichtung aufgenommen, die oder den Sächsischen Datenschutz- und Transparenzbeauftragten zu der Verwaltungsvorschrift anzuhören.

Vorbemerkung zu den §§ 80, 80a bis 80c

Mit den Regelungen wird der Rechtsrahmen für die Zulässigkeit der Fortspeicherung von personenbezogenen Daten über das jeweilige konkrete Ausgangsverfahren hinaus bestimmt.

In diesem Zusammenhang bestand Bedarf sowohl das Urteil des Bundesverfassungsgerichts vom 1. Oktober 2024, 1 BvR 1160/19, Bundeskriminalamtgesetz II, als auch das Urteil des Sächsischen Verfassungsgerichtshofs vom 25. Januar 2024, Vf. 91-II-19 umzusetzen.

Das Bundesverfassungsgericht hat in dem Grundsatzurteil vom 1. Oktober 2024 dargelegt, dass die vorsorgende Speicherung regelhaft eine zweckändernde Weiterverarbeitung darstelle für deren verfassungsrechtliche Rechtfertigung es einer Rechtsgrundlage bedürfe. Weiterhin müsse der Gesetzgeber angemessene Speicherzwecke und Speicherschwellen sowie eine angemessene Speicherdauer bestimmen (BVerfG, a. a. O., Rz. 181f). Der Gesetzgeber sei insbesondere gefordert, ein hinreichend ausdifferenziertes Regelungskonzept zur Speicherdauer zu formulieren (BVerfG, a. a. O., Rz. 200). Zwar ist Adressat dieses Urteils der Bund und betrifft dieses „nur“ die gesetzliche Regelung zur vorsorgenden Speicherung von personenbezogenen Daten im polizeilichen Informationsverbund. Aus den grundlegenden Ausführungen des Bundesverfassungsgerichts zur vorsorgenden Speicherung und zum Grundrecht auf informationelle Selbstbestimmung ist jedoch abzuleiten, dass die Ausführungen des Gerichts zu den Anforderungen an eine vorsorgende Speicherung und des insoweit bestehenden Regelungsauftrags, den der Gesetzgeber zu erfüllen habe, gleichermaßen Maßstab für die vorsorgende Speicherung in polizeilichen Landes-Informationssystemen bilden. Ein gesetzgeberischer Umsetzungsbedarf besteht daher auch dann, wenn die vorsorgende Datenverarbeitung nur in technischen Systemen erfolgt, auf die „nur“ die Bediensteten einer Landespolizei Zugriff haben. Vor diesem Hintergrund besteht Regelungsbedarf für eine spezifische Befugnisregelung zur vorsorgenden Speicherung, die ins-

besondere dem potentiell hohen Eingriffsgewicht der vorsorgenden Speicherung nach Herkunft der Daten (Rz. 159), der Eingriffsintensität der Datenerhebung insbesondere im Hinblick auf eine verhältnismäßige Ausgestaltung einer Speicherschwelle und der Speicherdauer differenzierend Rechnung trägt.

Das Eingriffsgewicht einer vorsorgenden Speicherung werde wesentlich geprägt durch:

- Art und Umfang der Daten (BVerfG, a. a. O., Rz. 160),
- dem Gewicht des vorausgegangenen Datenerhebungseingriffs (BVerfG, a. a. O., Rz. 159),
- insbesondere welchen Anlass die betroffene Person zu einer Speicherung gegeben hat (BVerfG, a. a. O., Rz. 161 objektiver Rechtsverstoß - Beschuldigter oder nur verdächtige Person),
- der denkbaren Verwendung von Daten und der damit verbundenen Folgen für den Betroffenen und schließlich
- der Speicherdauer (BVerfG, a. a. O., Rz. 164).

Dem potentiell hohen Eingriffsgewicht einer vorsorgenden Speicherung müsse der Gesetzgeber begegnen und den Staatsinteressen (Sicherheit) und Grundrechtsschutz des Bürgers (Achtung und Würde und Eigenwert) in einer gesetzlichen Regelung angemessen Rechnung tragen (BVerfG, a. a. O., Rz. 91). Die vorsorgende Speicherung stelle eine Zweckänderung dar. Eine solche bedürfe als Grundrechtseingriff einer gesetzlichen Grundlage (BVerfG, a. a. O., Rz. 181). Für eine verfassungsrechtliche Rechtfertigung bedürfe die vorsorgende Speicherung der Festlegung angemessener Speicherzwecke und Speicherschwellen sowie der Bestimmung einer angemessenen Speicherdauer (BVerfG, a. a. O., Rz. 182). Bei der Speicherung von Daten für die Verhütung und Verfolgung vom Speicherzweck erfasster Straftaten sei dies nur gegeben, wenn eine hinreichende Wahrscheinlichkeit dafür bestehe, dass die Betroffenen eine strafrechtlich relevante Verbindung zu möglichen Straftaten aufweisen und gerade die gespeicherten Daten zu deren Verhütung oder Verfolgung angemessen beitragen können. Diese Prognose müsse sich auf zureichende tatsächliche Anhaltspunkte stützen (BVerfG, a. a. O., Rz. 186). Als taugliche Prognosekriterien können insbesondere die Art, Schwere und Begehungsweise der vormaligen Straftat sowie der Persönlichkeit des Betroffenen und sein bisheriges strafrechtliches Erscheinungsbild in Frage kommen. Ferner ob die betroffene Person wiederholt und in welchem Ausmaß sie straffällig geworden ist (BVerfG, a. a. O., Rz. 186).

Die vorsorgende Speicherung dürfe zudem nicht zu einer Umgehung der verfassungsrechtlichen Anforderungen an eine zweckändernde Weiternutzung von personenbezogenen Daten führen (BVerfG, a. a. O., Rz. 191).

Im Kontext der bisherigen Regelungen des Sächsischen Polizeivollzugsdienstgesetzes zur vorsorgenden Speicherung hatte der Sächsische Verfassungsgerichtshof die Vorschrift des bisherigen § 80 Absatz 2 Nummer 1, 2 und 4 SächsPVDG für nicht normenklar und daher nicht verfassungsgemäß beurteilt. Die Anforderungen an die Normenklarheit bedingen, dass für den betroffenen Bürger anhand des Inhalts der Norm beurteilungsfähig sein muss, unter welchen Voraussetzungen eine Weiterverarbeitung seiner im Rahmen repressiver Maßnahmen gewonnenen personenbezogenen Daten über das Ausgangsverfahren hinaus zulässig ist. Aufgrund der bestehenden Regelungstechnik sei aber unklar, ob für die Weiterverarbeitung von vorsorgend gespeicherten Daten nach § 80 Absatz 2 SächsPVDG, die Anforderungen des § 79 Absatz 2 mit zu prüfen sind, somit zusätzlich gelten (SächsVerfGH, a. a. O., Seite 121f).

Die Regelung (neu) enthält in Absatz 1 die Befugnis zur vorsorgenden Speicherung von aus repressiven Maßnahmen erhobenen personenbezogenen Daten zu Verurteilten, Beschuldigten, Verdächtigen und Anlasspersonen zur künftigen Verhütung oder Verfolgung von Straftaten und bestimmt gemäß den Anforderungen des Bundesverfassungsgerichts die maßgeblichen Kriterien für die erforderliche tatsächengestützte Prognoseprüfung, in deren Ergebnis die Zulässigkeit der vorsorgenden Speicherung im Einzelfall vorliegen können. Absatz 2 bestimmt den Rahmen der Datenspeicherung je nach Personenkategorie und damit nach dem jeweiligen Anlass, den die betroffene Person für die Speicherung gegeben hat. Absatz 3 beinhaltet unter dem Aspekt „Regelungszusammenhang“ die bisher in § 80 Absatz 4 enthaltene sofortige Lösungsverpflichtung (Ablehnung Eröffnung des Hauptverfahrens, nicht nur vorläufige Verfahrenseinstellung). Absatz 4 enthält durch die Verweisung auf § 79a Absatz 2 den rechtlichen Rahmen, der Voraussetzung für die zweckändernde Weiternutzung der Daten ist.

Absatz 1

In Absatz 1 wird die bisherige Regelung aus § 80 Absatz 2 überführt und dahingehend geändert, dass die Anforderung der Prognose der künftigen Begehung einer Straftat (sog. Negativprognose) Voraussetzung der vorsorgenden Speicherung repressiv erhobener oder erlangter Daten sowohl von Verurteilten und Beschuldigten als auch von Verdächtigen ist. Für die Kategorie der Anlasspersonen bleibt es im Hinblick auf die vorsorgende Speicherung personenbezogener Daten bei der abweichenden Prognoseprüfung. Der Wortlaut der Regelung stellt klar, dass die vorsorgende Speicherung erforderlich sein muss. In Umsetzung der Rechtsprechung des Bundesverfassungsgerichts wird anstelle des bisherigen Begriffs „weiterverarbeiten“ der spezifische Begriff der „vorsorgenden Speicherung“ übernommen. Das Bundesverfassungsgericht hat in dem genannten Grundsatzurteil eine Speicherung als „vorsorgend“ bezeichnet, wenn sie nicht zum Zweck ihrer Erhebung oder Herstellung erfolgt, ohne dass eine neue Zweckbindung, die zu einer unmittelbaren weiteren Nutzung führt, an ihre Stelle gesetzt wird. Die neu gesetzten Zwecke liegen in der Bereithaltung der Daten für den Fall, dass sie für konkrete Zwecke künftig benötigt werden (BVerfG, a. a. O, Rz. 158).

Auch im Gesetzentwurf des Bundes zur Umsetzung des Urteils des BVerfG im Bundeskriminalamtgesetz (BT Drs. 21/234) wird im Hinblick auf die bevorratende Speicherung im Informationsverbund der neue Begriff der vorsorgenden Speicherung geführt (siehe Gesetzentwurf, § 30a Absatz 2 BKAG-neu). Aus Gründen der Harmonisierung und der Anwenderfreundlichkeit ist daher analog zu formulieren.

Absatz 2

Die Regelung in Absatz 2 bestimmt den zulässigen Datenkranz der vorsorgenden Speicherung nach Personenkategorien unter Berücksichtigung des Anlasses, den die betroffene Person für die Speicherung gegeben hat. Zur näheren Eingrenzung des Datenkranzes wird in den Nummern 1 und 2 an die Regelungen der BKA-Datenverordnung angeknüpft.

Absatz 3

Die Regelung überführt den Regelungsinhalt des § 80 Absatz 4 zur Pflicht zu unverzüglichen Löschung, soweit die Eröffnung des Hauptverfahrens unanfechtbar abgelehnt wird oder das Verfahren nicht nur vorläufig eingestellt wurde. Aufgrund der Wertigkeit dieser datenschutzrechtlichen Verpflichtung zur Löschung wird der bisherige Regelungsstandort beibehalten und nicht in den (eigentlich zutreffenden) Regelungszusammenhang des § 91 Absatz 3 gestellt.

Absatz 4

Absatz 4 bestimmt, dass für die weitere Verarbeitung der vorsorgend gespeicherten Daten die rechtlichen Anforderungen des § 79a Absatz 2 gelten. Das Bundesverfassungsgericht

hatte hierzu formuliert, dass unerlässliche Voraussetzung für die Verfassungsmäßigkeit der Speicherbefugnis weiterhin klar normierte Verwendungsregeln sind, die insbesondere den im Urteil des Bundesverfassungsgerichts vom 20. April 2016, 1 BvR 966/09, formulierten verfassungsrechtlichen Anforderungen an die zweckändernde Weiterverarbeitung personenbezogener Daten genügen müssen (siehe Urteil, a. a. O., Rz. 189). Mit der Regelung wird zugleich die Vorgabe des Sächsischen Verfassungsgerichtshofs umgesetzt, durch normklare Regelung sicherzustellen, dass für den betroffenen Bürger anhand des Inhalts der Norm beurteilungsfähig ist, unter welchen Voraussetzungen eine Weiterverarbeitung seiner im Rahmen repressiver Maßnahmen gewonnenen personenbezogenen Daten über das Ausgangsverfahren hinaus zulässig ist.

§ 80a

Die Regelung (neu) enthält in Absatz 1 die Befugnis zur vorsorgenden Speicherung von aus repressiven Maßnahmen erhobenen personenbezogenen Daten zu Zeugen, Opfern, Hinweisgebern und Kontakt- und Begleitpersonen, soweit dies zu Zwecken der künftigen Verhütung oder Verfolgung von Straftaten erforderlich ist. Die Regelung in Absatz 1 entspricht der bisherigen Regelung des § 80 Absatz 3.

Absatz 1

Satz 1 enthält die bisherige Regelung des § 80 Absatz 3 Satz 1.

Satz 2 bestimmt, dass eine Speicherung von Personen nach Satz 1 Nummer 1 bis 3 ohne Einwilligung nur erfolgen darf, wenn anderenfalls der Speicherungszweck gefährdet werden würde und entspricht der bisherigen Regelung von § 80 Absatz 3 Satz 3. Satz 3 entspricht der bisherigen Regelung des § 80 Absatz 3 Satz 2, dass eine Speicherung der Personen nach Absatz 1 Nummer 1 bis 3 grundsätzlich der Einwilligung der betroffenen Personen bedarf.

Absatz 2

Die Regelung in Absatz 2 bestimmt den zulässigen Datenkranz der vorsorgenden Speicherung und unterscheidet nach dem Anlass den die betroffenen Personenkategorien für die Speicherung gegeben haben. Zur näheren Eingrenzung des Datenkranzes wird an die Regelungen der BKA-Datenverordnung angeknüpft.

§ 80b

Mit der Regelung wird eine spezifische Rechtsgrundlage für die vorsorgende Speicherung von zu Gefahrenabwehrzwecken erhobenen personenbezogenen Daten zu Zwecken der künftigen Gefahrenabwehr (Absatz 1 Nummer 1) oder zu Zwecken der künftigen Strafverfolgung (Absatz 1 Nummer 2) geschaffen.

Satz 1 Nummer 1 bildet die Regelung für die vorsorgende Speicherung von Personen zu denen die tatsächengestützte Prognose einer künftigen (Selbst-) Gefährdung besteht. Satz 1 Nummer 2 bildet die Rechtsgrundlage für die vorsorgende Speicherung von Personen, bei denen aufgrund von präventiv erhobenen oder erlangten polizeilichen Erkenntnissen die tatsächengestützte Prognose besteht, dass die betroffene Person künftig Straftaten von erheblicher Bedeutung begeht. Die vorsorgende Speicherung der zu präventiven Zwecken erhobenen Daten zu den betroffenen Personen erfolgte bisher über die Weiterverarbeitungsgeneralklausel des bisherigen § 80 Absatz 1.

In der polizeilichen Praxis besteht das Erfordernis, zu präventiven Zwecken erhobene personenbezogene Daten zu Personen vorsorgend zu speichern, zu denen vorliegende polizeiliche Erkenntnisse die Prognose einer künftigen (Selbst-)Gefährdung der Person begründen. Praktische Anwendungsfälle sind insbesondere Suizidenten, Personen, die aufgrund

einer Erkrankung (beispielsweise Demenz) orientierungslos sind oder sog. Dauer-Ausreißer, Kinder oder Jugendliche, die wiederholt von zu Hause „ausreißen“. Zum Zweck der Abwehr künftiger Gefahren ist die vorsorgende Speicherung personenbezogener Daten zu diesen Personen erforderlich (Satz 1 Nummer 1). Satz 1 Nummer 2 bildet die analoge Rechtsgrundlage für die vorsorgende Speicherung von Anlasspersonen gemäß § 80 Absatz 1 Nummer 4, soweit die Datenerhebung auf der Grundlage dieses Gesetzes erfolgt ist. Wie bei § 80 Absatz 1 Nummer 4 ist Voraussetzung für die vorsorgende Speicherung, dass eine tatsächengestützte Prognose der künftigen Begehung von Straftaten von erheblicher Bedeutung durch die betreffende Person begründet ist.

Satz 2 bestimmt, welche Daten zu den Personen nach Absatz 1 Nummer 1 und 2 jeweils gespeichert werden dürfen.

Absatz 2

Die Regelung bestimmt, welche Anforderungen an die weitere Verwendung der nach Absatz 1 vorsorgend gespeicherten personenbezogenen Daten gelten.

§ 80c

Mit der Regelung (neu) wird eine Rechtsgrundlage für die vorsorgende Speicherung von personenbezogenen Daten von Erziehungsberechtigten, Vormündern und Bewährungshelfern in das Sächsische Polizeivollzugsdienstgesetz aufgenommen.

Satz 1 bezeichnet den Personenkreis, dessen Daten im Zusammenhang mit einer vorsorgenden Speicherung von Daten einer Person nach § 80, § 80a, § 80b vorsorgend gespeichert werden können.

Satz 2 bestimmt, dass die vorsorgende Speicherung der personenbezogenen Daten sonstiger Personen nicht recherchefähig erfolgen darf. Hiervon ist allein die Recherchefähigkeit im Hinblick auf den Zweck der vorsorgenden Speicherung umfasst; andere Speicherzwecke fallen hingegen nicht unter die Regelung. Damit wird sichergestellt, dass ein Abruf personenbezogener Daten der sonstigen Person allein über einen Datenabruf der Person erfolgen darf, zu der die Speicherung der sonstigen Person erforderlich war. Durch die technische Gestaltung der Systeme ist sicherzustellen, dass nach sonstigen Personen nicht unmittelbar recherchiert werden kann. Satz 3 bezeichnet die personenbezogenen Daten, die zu sonstigen Personen gespeichert werden dürfen, abschließend. Satz 4 regelt durch den Verweis auf § 79a, welche rechtlichen Anforderungen für die Weiterverarbeitung der Daten gelten.

§ 80d

Das Bundesverfassungsgericht hat in dem Urteil vom 1. Oktober 2024, 1 BvR 1160/19, im Kontext der Ausführungen zur vorsorgenden Speicherung formuliert, dass es für die verfassungsrechtliche Rechtfertigung der vorsorgenden Speicherung personenbezogener Daten zudem der gesetzlichen Regelung einer angemessenen Speicherdauer bedürfe (Rz. 187). Die verfassungsrechtlich gebundene kompensatorische Einhegung einer Befugnis zur vorsorgenden Speicherung gebiete ein Regelungskonzept, dass differenzierte Prüfungs- und Aussonderungsfristen setzt. Auch muss die vorsorgende Speicherung grundsätzlich begrenzt werden (Rz. 184, 187).

In Umsetzung der Rechtsprechung des Bundesverfassungsgerichts werden durch die Regelungen in § 80d sowohl allgemeine Kriterien (Absatz 2) für die Bestimmung von Aussonderungsprüffristen für die vorsorgende Speicherung bestimmt als auch ein gesetzlicher Rahmen (Absatz 3) für Aussonderungsprüffristen für vorsorgend gespeicherte Daten vorgegeben, der nach Personenkategorien, Schwere der Straftat und Alter der betroffenen Person unterscheidet.

Die Vorschrift beinhaltet daneben erforderliche Regelungen zum Fristbeginn der Aussonderungsprüffrist für die Verarbeitung von Daten für die konkreten Zwecke, zu denen die Erhebung erfolgte (Absatz 1 Satz 5 3 Satz 2) und zur möglichen Verlängerung einer Aussonderungsprüffrist und trifft Regelungen zur Höchstspeicherfrist (Absatz 4).

Absatz 1

Satz 1 (neu) enthält den Grundsatz, dass für die Zulässigkeit der Dauer der Speicherung personenbezogener Daten zum Zweck der Erfüllung einer bestimmten Aufgabe Maßstab die Erforderlichkeit des Datums für die konkrete Aufgabenerfüllung ist. Die Sätze 2 bis 4 beinhalten die bisher in § 91 Absatz 3 Sätze 1, 2 und 4 enthaltenen Regelungen, um durch den rechtssystematischen Zusammenhang die Verständlichkeit der Regelungen (wann ist besteht eine Verpflichtung zur Löschung) sicherzustellen. Satz 2 bestimmt die Anforderungen an die Zulässigkeit der Speicherung und der Dauer der Speicherung von für eine konkrete Aufgabe und für einen bestimmten Zweck erhobenen oder erlangten Daten. Hierfür wird als Maßstab für die Speicherung und die Dauer der Speicherung der Grundsatz der Erforderlichkeit der (weiteren) Speicherung für die jeweilige konkrete Aufgabenerfüllung vorausgesetzt. Satz 3 überführt den bisherigen Regelungsinhalt von § 91 Absatz 3 Satz 3, wonach durch festzulegende Prüffristen sicherzustellen ist, dass die Erforderlichkeit der weiteren Speicherung der Daten für die konkrete Aufgabenerfüllung zu überprüfen ist. Satz 4 überführt den bisherigen Regelungsinhalt von § 91 Absatz 3 Satz 4 und bestimmt abweichend von der bisherigen Regelung kurze Aussonderungsprüffristen gestaffelt nach Erwachsenen (fünf Jahre, bisher zehn Jahre, Jugendliche (drei Jahre, bisher fünf Jahre) und Kinder (zwei Jahre) und bestimmt den Beginn des Fristlaufs mit Kenntniserlangung durch die Polizei. Satz 5 sieht ein Dokumentationserfordernis für den Fall vor, dass im Rahmen der Aussonderungsprüfung festgestellt wird, dass die Daten weiterhin zur Aufgabenerfüllung erforderlich sind und somit noch nicht gelöscht werden können. Zu dokumentieren sind hierbei die Gründe sowie die konkrete Dauer der weiteren Speicherung.

Absatz 2

Die Regelung beinhaltet die allgemeinen Kriterien, die die Polizei bei der Bestimmung von Aussonderungsprüffristen im Hinblick auf vorsorgend gespeicherte Daten anzuwenden hat.

Absatz 3

Satz 1 Nummer 1 bis 3 enthält gestaffelt nach Schwere der Straftat, dem Anlass, den die betroffene Person für die Speicherung gesetzt hat (Verurteilter, Beschuldigter, Verdächtiger) und dem Alter (Erwachsene, Jugendliche, Kinder) Regelungen zu dem maximalen Aussonderungsprüffristen.

Nummer 1 bestimmt den maximalen Rahmen für die im Einzelfall festzulegende Aussonderungsprüffrist von Verurteilten. Diese beträgt zehn Jahre bei Erwachsenen und fünf Jahre bei Jugendlichen. Kinder fallen aufgrund des Umstands, dass diese mangels Strafmündigkeit nicht „Verurteilte“ und nicht „Beschuldigte“ im Sinne der Vorschrift sein können, nicht unter die Regelung. Die Regelung überführt die bisherige Frist aus § 91 Absatz 3 Satz 4.

Nummer 2 bestimmt als maximalen Rahmen für die im Einzelfall festzulegende Aussonderungsprüffrist von Beschuldigten unter Berücksichtigung der Schwere der Straftat und des Alters der betroffenen Person. Auch Nummer 2 findet auf die Personengruppe der Kinder aufgrund der bestehenden Strafunmündigkeit keine Anwendung.

Nummer 3 bestimmt die maximalen Aussonderungsprüffristen für die Personengruppe der Verdächtigen unter Berücksichtigung der Schwere der Straftat und des Alters der betroffenen Person. Im Gegensatz zu Nummer 1 und Nummer 2 sind in Nummer 3 auch Kinder ab dem siebten Lebensjahr zu berücksichtigen. Auch Kinder können einer Straftat verdächtig sein, ohne dass hierfür eine Anknüpfung an die Strafmündigkeit erfolgen muss.

Nummer 4 trifft im Hinblick auf den Personenkreis der Anlasspersonen nach § 80 Absatz 1 Nummer 4 und § 80b Absatz 2 eine nach Alter gestaffelte maximale Aussonderungsprüffrist. Auch Kinder können Anlasspersonen sein. Daher werden diese ab dem siebten Lebensjahr in die Regelung mit einbezogen.

Nummer 5 regelt die maximalen Aussonderungsprüffristen für Zeugen, Opfer, Hinweisgeber und überführt die bisherige Regelung aus § 91 Absatz 4 Sätze 4 bis 7 und unterscheidet zwischen einwilligungsbasierter vorsorgender Speicherung und vorsorgender Speicherung ohne Einwilligung.

Nummer 6 bestimmt die maximalen Aussonderungsprüffristen für Kontakt- und Begleitpersonen (siehe Begriffsbestimmung in § 4 Nummer 9) und unterscheidet bei der Fristlänge insbesondere nach der Schwere der Straftat der „anderen Person“ im Sinne der Begriffsbestimmung in § 4 Nummer 9.

Nummer 7 bestimmt die maximalen Aussonderungsprüffristen für vorsorgende Speicherung von durch präventive Maßnahmen erhobene personenbezogene Daten zu gefährdeten, hilflosen oder vermissten Personen gemäß § 80b Absatz 1 gestaffelt nach Alter.

Nummer 8 bestimmt die maximalen Aussonderungsprüffristen für die vorsorgende Speicherung von sonstigen Personen nach § 80c.

Satz 2 regelt im Hinblick auf Erstspeicherungen von Verdächtigen oder Beschuldigten von schweren Straftaten nach § 100a Absatz 2 der Strafprozessordnung (Nummer 2a) kürzere Aussonderungsprüffristen.

Satz 3 bestimmt als Fristbeginn für die Aussonderungsprüffristen den Tag, an dem die vorsorgende Speicherung erfolgt ist und überführt die Ausnahmeregelung des § 91 Absatz 3 Satz 10.

Absatz 4

Absatz 4 enthält in Satz 1 die Anforderungen an die Verlängerung einer Aussonderungsprüffrist und sieht eine solche nur dann vor, wenn weiterhin relevante Umstände vorliegen, die die Verlängerung der Aussonderungsprüffrist begründen können, oder wenn neue für die Bestimmung der Aussonderungsprüffrist relevante Umstände hinzugetreten sind. Sätze 2 und 3 bestimmen schließlich Höchstspeicherfristen im Hinblick auf „sonstige Straftaten“ und für die Speicherung von Zeugen, Opfern, Hinweisgebern bei Nichtvorliegen der Einwilligung.

Absatz 5

In Absatz 5 wird von der durch das Bundesverfassungsgericht eingeräumte Delegationsbefugnis (siehe Urteil, a. a. O., Rz. 190) Gebrauch gemacht und das Sächsische Staatsministerium des Innern verpflichtet, durch mit der oder dem Sächsischen Datenschutz- und Transparenzbeauftragten abzustimmenden Verwaltungsvorschrift Näheres, insbesondere zu von der vorsorgenden Speicherung ausgenommenen personenbezogenen Daten (beispielsweise „Bagatelldeliktstrafaten“), zu den Anforderungen an die erforderliche Prognoseprüfung der vorsorgenden Speicherung und die Bestimmung und Verlängerung von Aussonderungsprüffristen im Einzelfall, die Lösungsverpflichtungen und insbesondere an die Dokumentationspflichten zu den Entscheidungen gemäß den §§ 80 bis 80c, § 80d und § 91 zu bestimmen und schließlich an die technisch und organisatorischen Vorkehrungen zur Einhaltung der bezeichneten Anforderungen.

Zu Nummer 29

Zu Buchstabe a

Die Änderung dient der Korrektur eines redaktionellen Versehens.

Zu Buchstabe b

Gemäß § 108 Absatz 4 Satz 2 ist die Regelung des § 81 Absatz 4 Satz 2 am 31. Dezember 2025 außer Kraft getreten. In Konsequenz des Außerkrafttretens wird die Regelung gestrichen.

Zu Nummer 30

§ 83

Die Änderungen dienen der Korrektur eines redaktionellen Versehens.

§ 84

Absatz 1

Satz 1 regelt die Zulässigkeit der Übermittlung personenbezogener Daten an andere Polizeidienststellen der Länder und des Bundes zum Zweck der eigenen Aufgabenerfüllung. Soweit die Datenübermittlung zur eigenen Aufgabenerfüllung erfolgt, handelt es sich um Datenverarbeitung im Rahmen der Zweckbindung. Maßstab für die Zulässigkeit der Datenweiterverarbeitung ist daher allein § 79a Absatz 1 SächsPVDG.

Satz 2 regelt demgegenüber die Zulässigkeit von Datenübermittlungen an andere Polizeidienststellen der Länder und des Bundes, die zur Erfüllung der Aufgaben der empfangenden Stelle erforderlich sind. Hierbei handelt es sich um eine zweckändernde Datenverarbeitung, sodass in derartigen Fällen die Voraussetzungen des § 79a Absatz 2 und 4 beachtet werden müssen.

Absatz 2

Satz 1 Nummer d

Zweck der ergänzenden Regelung ist es, eine Datenübermittlungsbefugnis in das Sächsische Polizeivollzugsdienstgesetz aufzunehmen, die es der Polizei erlaubt, personenbezogene Daten an eine öffentliche Stelle zu übermitteln, die keine Gefahrenabwehrbehörde ist. Die Befugnisregelung setzt ein Datenübermittlungsersuchen der betreffenden öffentlichen Stelle voraus, ferner, dass die Zulässigkeit des Datenübermittlungsersuchens der öffentlichen Stelle, die um Datenübermittlung ersucht, bereichsspezifisch geregelt ist und dass die Datenübermittlung für die Aufgabenerfüllung der jeweiligen öffentlichen Stelle erforderlich ist. Für die neue Regelung besteht erheblicher praktischer Bedarf. Anwendungsfälle sind Datenübermittlungsersuchen der Finanzbehörden oder der Gerichtsvollzieher im Zusammenhang mit erforderlichen Vollstreckungstätigkeiten. Polizeiliche Erkenntnisse zu möglichen, von betroffenen Personen für die Bediensteten ausgehende Gefahren, können zum Zweck der Aufgabenerfüllung erforderlich sein. Mit der Ergänzung wird eine bestehende Regelungslücke unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts zur Ausgestaltung von Datenübermittlungsregelungen (sog. „Doppeltür-Entscheidung“ des BVerfG, Beschluss vom 27. Mai 2020, 1 BvR 1873/13, 1 BvR 2618/13, Bestandsdatenauskunft II, Rz. 130) geschlossen.

Satz 2 greift die Regelung des Absatz 1 wieder auf, wonach hinsichtlich notwendiger Übermittlungen personenbezogener Daten nach Satz 1 danach zu unterscheiden ist, ob es sich um solche handelt, die der eigenen polizeilichen Aufgabenerfüllung dienen oder für die Erfüllung der Aufgaben der empfangenden Stelle erforderlich sind. Erfolgt die Datenübermittlung für die Erfüllung eigener Aufgaben, sind die Voraussetzungen des § 79a Absatz 1 zu

beachten. Datenübermittlungen zur Aufgabenerfüllung der empfangenden Stelle richten sich aufgrund des zweckändernden Charakters nach § 79a Absatz 2 und 4.

Absatz 3

Die Änderungen in Satz 1 stellen redaktionelle Folgeänderungen dar.

Mit der Ergänzung unter Nummer 4 und in Satz 3 wird zum Zweck der Bekämpfung häuslicher Gewalt eine Befugnisregelung aufgenommen, die es der Polizei erlaubt, die Kontaktdaten von Personen, die häuslicher Gewalt ausgesetzt sind, an geeignete Beratungsstellen nichtbehördlicher Organisationen zu übermitteln.

Häusliche Gewalt in diesem Sinne beinhaltet alle Formen körperlicher, sexuelle oder psychischer Gewalt und umfasst familiäre sowie partnerschaftliche Gewalt. Häusliche Gewalt liegt vor, wenn die Gewalt zwischen Personen stattfindet, die in einer familiären oder partnerschaftlichen Beziehung zusammenwohnen. Sie liegt auch vor, wenn sie unabhängig von einem gemeinsamen Haushalt innerhalb der Familie oder in aktuellen oder ehemaligen Partnerschaften geschieht (siehe die Definition im Bundeslagebild des Bundeskriminalamts zu häuslicher Gewalt 2023, S. 1). Durch die Regelung soll proaktiv eine Kontaktaufnahme mit der betroffenen Person zum Zweck der Beratung ermöglicht werden. Die Eignung der Beratungsstellen ist durch das Sächsische Staatsministerium für Soziales, Gesundheit und Gesellschaftlichen Zusammenhalt zu bestimmen. Ziel der Regelungen in den Sätzen 3 und 4 ist es, die datenschutzrechtlichen Interessen der betroffenen Person zu wahren.

Nummer 5 sieht darüber hinaus die Möglichkeit vor, auch die Daten der volljährigen Person, von der die häusliche Gewalt ausgeht, an geeignete Beratungsstellen zu übermitteln, um ein weiteres Auftreten von häuslicher Gewalt zu verhüten. Auch hierfür ist jedoch die Eignung der jeweiligen Beratungsstelle durch das Sächsische Staatsministerium für Soziales, Gesundheit und Gesellschaftlichen Zusammenhalt festzustellen. Ziel ist hierbei eine frühzeitige Täterintervention, die direkt im Anschluss an eine Straftat oder einen Verdachtsfall erfolgen soll. Somit können dem Täter in unmittelbaren zeitlichen Zusammenhang mit der vorangegangenen Tathandlung professionelle Unterstützungsangebote unterbreitet werden.

Absatz 3 Satz 2 greift die Regelung des Absatz 1 sowie des Absatzes 2 Satz 2 wieder auf, wonach hinsichtlich notwendiger Übermittlungen personenbezogener Daten nach Satz 1 danach zu unterscheiden ist, ob es sich um solche handelt, die der eigenen polizeilichen Aufgabenerfüllung dienen oder für die Erfüllung der Aufgaben der empfangenden Stelle erforderlich sind. Erfolgt die Datenübermittlung für die Erfüllung eigener Aufgaben, sind die Voraussetzungen des § 79a Absatz 1 zu beachten. Datenübermittlungen zur Aufgabenerfüllung der empfangenden Stelle richten sich aufgrund des zweckändernden Charakters nach § 79a Absatz 2 und 4.

Absatz 5

Die Änderung stellt eine redaktionelle Folgeänderung dar.

§ 84a

Mit der Regelung wird eine Rechtsgrundlage für eine öffentliche Fahndung nach Personen zum Zweck der Ermittlung der Identität der Person oder des Aufenthaltsorts der Person zur Abwehr von Gefahren für die betreffende Person (Nummer 1) oder von der betroffenen Person (Nummer 2) in das Sächsische Polizeivollzugsdienstgesetz aufgenommen und damit eine bestehende Regelungslücke geschlossen.

Zu Nummer 31

§ 86

Die geltende Vorschrift bezieht sich begrifflich allein auf die Aufzeichnung von Anrufen im Notfall. Sie deckt nicht den polizeifachlichen Bedarf ab, andere Kommunikation (beispielsweise über eine Notruf-App) und den Standort des Anrufers bei Anwahl der Notrufnummer 110 zu erheben. Gemäß § 164 Absatz 1 des Telekommunikationsgesetzes (TKG) vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 35 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, sind Notrufverbindungen jederzeit unverzüglich zu der örtlich zuständigen Notrufabfragestelle herzustellen. Nach § 2 Nummer 2 der Verordnung über Notrufverbindungen (NotrufV) vom 6. März 2009 (BGBl. I S. 481), die zuletzt durch Artikel 34 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, ist „Notrufabfragestelle“ die nach Landesrecht zuständige Stelle zur Entgegennahme von Notrufen. Gemäß § 164 Absatz 3 TKG ist hierbei zu berücksichtigen, dass bei Gewährleistung einer gleichwertigen Notrufoffkommunikation von Menschen mit Behinderungen im Rahmen von Notrufverbindungen von der Polizei zukünftig nicht nur Sprache, sondern auch Text und gegebenenfalls Video im Rahmen der Notrufoffkommunikation zu verarbeiten sind.

Absatz 1

Mit dem neuen Absatz 1 wird eine Rechtsgrundlage für den Abruf von Standortdaten geschaffen, die nach Anwahl der Notrufnummer 110 mittels eines Smartphones automatisiert und ohne Interaktion der anrufenden Person anfallen. Mit der Formulierung „einschließlich der den Notruf begleitenden personenbezogenen Daten“ wird geregelt, dass die gesamte Kommunikation (Chatverläufe bei Notruf-App) verarbeitet werden darf, soweit dies für die Abwehr von Gefahren oder für die Verhütung von Straftaten erforderlich ist.

Absatz 2

Die Regelung entspricht der Bisherigen in § 86 Absatz 1 Satz 2.

Absatz 3

Die Regelung in Satz 1 entspricht der Bisherigen in § 86 Absatz 1 Satz 3 mit der Änderung, dass aus Gründen der Verhältnismäßigkeit die Höchstspeicherfrist auf 30 Tage gekürzt wurde. Mit Satz 2 (neu) wird klargestellt, dass Aufzeichnungen auch zu Zwecken der Aus- und Fortbildung genutzt werden dürfen.

Zu Nummer 32

§ 88

Die UEFA EURO 2024 hat gezeigt, dass ein polizeifachlicher Bedarf besteht, neben der Einbeziehung von bestehenden polizeilichen Datenbeständen (polizeilicher Informationsverbund) weitere Datenbestände bei der Durchführung von Zuverlässigkeitsüberprüfungen zu berücksichtigen. Erforderlich ist es, den aktuellen Datenbestand der Wohnsitz-Landeskriminalämter der letzten fünf Jahre einzubeziehen, aber auch Daten des Ausländerzentralregisters, des Landesamtes für Verfassungsschutz oder bei Personen mit Wohnsitz im Ausland, Daten der Polizeibehörden des jeweiligen Staates. Aufgrund zunehmender Digitalisierung besteht zudem Bedarf, Zuverlässigkeitsüberprüfungen im elektronische Verfahren zu ermöglichen. Das Verfahren der Zuverlässigkeitsüberprüfung bedingt eine Vielzahl von Datenverarbeitungsschritten, ohne dass dies der bestehenden Vorschrift klar entnommen werden konnte. Durch die neue Regelung sollen die erforderlichen Datenverarbeitungsregelungen umfassend geregelt werden. Es besteht zudem der polizeifachliche Bedarf, zum Zweck der Zuverlässigkeitsüberprüfung im elektronischen Verfahren die Identität der betroffenen Person zu überprüfen und Kopien des Personalausweises zum Vorgang zu nehmen.

Absatz 1

Die Regelung beinhaltet die Voraussetzungen, unter denen eine Zuverlässigkeitsüberprüfung erfolgen kann. Neben dem Erfordernis eines Ersuchens einer öffentlichen oder nicht-öffentlichen Stelle muss es sich bei der Veranstaltung um eine besonders gefährdete Veranstaltung handeln und die zu überprüfende Person muss einen privilegierten Zutritt zu der Veranstaltung haben. Durch die Anforderung des „privilegierten Zutritts“ soll sichergestellt werden, dass nur solche Personen überprüft werden, die aufgrund ihrer tatsächlichen „Nähe“ zu der Veranstaltung ein potientiellles Sicherheitsrisiko für die Veranstaltung bilden können.

Absatz 2

Satz 1 bestimmt die verfahrensrechtlichen Anforderungen an die Zuverlässigkeitsüberprüfung.

Satz 2 regelt die Anforderungen an die Datenschutzinformation der betroffenen Person, die vor der Zustimmungserteilung zu erfolgen hat.

Absatz 3

Die Regelung bestimmt, welche Datenbestände bei der Durchführung von Zuverlässigkeitsüberprüfungen einbezogen werden dürfen.

Absatz 4

Satz 1 beinhaltet die Rechtsgrundlage für die Datenübermittlung der Polizei an andere öffentliche Stellen zum Zweck der Datenerhebung. Satz 2 regelt die enge Zweckbindung für die durch die Polizei bei anderen öffentlichen Stellen erhobenen Daten und stellt die Einhaltung dieser insbesondere durch das Erfordernis einer separaten Speicherung sicher. Die Sätze 3 und 4 beinhalten die Rechtsgrundlage für die Übermittlung des Ergebnisses der Zuverlässigkeitsüberprüfung an die ersuchende öffentliche oder private Stelle. Satz 5 enthält die Verpflichtung zur Unterrichtung der betroffenen Person über das Ergebnis der Überprüfung.

Absatz 5

Die Regelung übernimmt zur Sicherstellung der Einhaltung der Zweckbestimmung der Datenverarbeitung bei der privaten oder öffentlichen Stelle den Regelungsinhalt aus § 88 Absatz 2.

Absatz 6

Die Regelung bestimmt eine Höchstspeicherfrist von sechs Monaten für die im Rahmen der Zuverlässigkeitsüberprüfung verarbeiteten personenbezogene Daten. Die Ausnahmeregelung von der Höchstspeicherfrist in Satz 2 sieht eine höhere Speicherdauer vor, wenn aufgrund des Ergebnisses der Zuverlässigkeitsüberprüfung ein Rechtsstreit zu erwarten oder bereits anhängig ist. Satz 3 beinhaltet die Regelung zum Beginn des Fristlaufs.

Absatz 7

In Absatz 7 wird die Regelung aus § 88 Absatz 2 zur Unterrichtung der Sächsischen Datenschutz- und Transparenzbeauftragten übernommen.

Zu Nummer 33

§ 89a

§ 89a dient der Umsetzung der Richtlinie (EU) 2023/977 des Europäischen Parlaments und des Rates vom 10. Mai 2023 über den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten und zur Aufhebung des Rahmenbeschlusses 2006/960/JI des Rates, soweit diese dem Landesgesetzgeber obliegt. Die Richtlinie trifft Vorgaben zum Informationsaustausch mit EU-Mitgliedstaaten und Schengen-assozierte Staaten zum Zweck der Verhütung, Aufdeckung oder Untersuchung von Straftaten. Ziel der bis zum 12. Dezember 2024 mitgliedstaatlich umzusetzenden Richtlinie ist eine Verbesserung des bestehenden Rechtsrahmens zum Informationsaustausch, um insbesondere auf grenzüberschreitende kriminelle Aktivitäten reagieren zu können.

Am 30. Januar 2025 hat die Europäische Kommission aufgrund unterbliebener Notifizierung der Umsetzung ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet. Auf Bundesebene wurden und werden daher zeitnah separate Gesetzgebungsvorhaben zur Umsetzung der Richtlinie im Bundeskriminalamtgesetz, im Bundespolizeigesetz und in weiteren Rechtsvorschriften initiiert.

Die Aufnahme des neuen § 89a erfolgt vor dem Hintergrund dieser Gesetzesinitiativen und der jüngsten Abstimmungen zwischen Bund und Ländern.

Absatz 1

Absatz 1 Satz 1 bestimmt den Anwendungsbereich des § 89a. Dieser ist auf den der Straftatenverhütung dienenden direkten Informationsaustausch im Sinne der Richtlinie (EU) 2023/977 – also Informationersuchen und die Übermittlung von Informationen – zwischen der Polizei und den zentralen Kontaktstellen, Polizeibehörden und sonstigen für die Verhütung oder Verfolgung von Straftaten zuständigen öffentlichen Stellen der EU-Mitgliedstaaten und der Schengen-assozierten Staaten beschränkt. Für diese Fälle treffen die Absätze 2 bis 8 des künftigen § 89a besondere Regelungen, die die allgemeinen Bestimmungen im Anwendungsbereich der Richtlinie (EU) 2023/977 ergänzen und vor allem in verfahrensbezogener Hinsicht präzisieren. Der auf die Straftatenverhütung gerichtete Informationsaustausch über das Bundeskriminalamt als zentrale Kontaktstelle der Bundesrepublik Deutschland richtet sich ausschließlich nach den Vorschriften des Bundeskriminalamtgesetzes, der Informationsaustausch zu Strafverfolgungszwecken zudem nach dem Gesetz über die internationale Rechtshilfe in Strafsachen. Es bedarf daher keiner landesrechtlichen Umsetzung der das Handeln der zentralen Kontaktstellen betreffenden Vorgaben der Richtlinie (EU) 2023/977.

Eine grundrechtsrelevante Erweiterung der Datenerhebungs- und -übermittlungsbefugnisse der Polizei ist mit diesen Regelungen nicht verbunden. § 89a geht lediglich insoweit über die Regelungen in § 89 hinaus, als er auch Vorgaben für den Austausch solcher Informationen macht, die keine personenbezogenen Daten darstellen. Zwar bedarf der Austausch solcher von vornherein nicht grundrechtsrelevanter Informationen nach der deutschen Grundrechtsdogmatik keiner gesetzlichen Regelung, gleichwohl erscheint eine solche zur mitgliedstaatlichen Umsetzung der Richtlinie (EU) 2023/977 – insbesondere dessen Artikel 4 Absatz 1 Satz 1, der eine Regelung durch Rechtsvorschrift verlangt – angezeigt. § 89a stellt zudem sicher, dass Informationen, die personenbezogene Daten darstellen, nur unter den Voraussetzungen des § 89 übermittelt werden dürfen.

Absatz 2

§ 89a setzt Artikel 4 Absatz 1 Satz 1 der Richtlinie (EU) 2023/977 um, indem er das Landeskriminalamt Sachsen auf Rechtsvorschriftenebene zu einer benannten Strafverfolgungsbehörde im Sinne des Artikels 2 Absatz 2 der Richtlinie (EU) 2023/977 bestimmt. Nur das Landeskriminalamt ist damit befugt, Informationersuchen an die zentralen Kontaktstellen anderer EU-Mitgliedstaaten oder Schengen-assoziierter Staaten zu richten. Absatz 2

Satz 2 dient der Umsetzung von Artikel 4 Absatz 4 und 5 der Richtlinie (EU) 2023/977, Absatz 2 Satz 3 der Umsetzung von Artikel 4 Absatz 6 und Absatz 2 Satz 4 der Umsetzung von Artikel 4 Absatz 1 Satz 4 der Richtlinie.

Absätze 3 bis 7

Absatz 3 dient der Umsetzung von Artikel 8 Absatz 2 der Richtlinie (EU) 2023/977.

Absatz 4 enthält eine Legaldefinition des Begriffs der Information und dient zu- dem der Umsetzung von Artikel 3 Buchstabe d der Richtlinie (EU) 2023/977.

Absatz 5 dient der Umsetzung von Artikel 1 Absatz 3 Buchstabe c und Artikel 7 Absatz 5 Buchstabe f der Richtlinie (EU) 2023/977.

Absatz 6 Satz 1 dient der Umsetzung von Artikel 7 Absatz 3 Satz 1 und 3 der Richtlinie (EU) 2023/977, Absatz 6 Satz 2 der Umsetzung von Artikel 7 Absatz 3 Satz 3 und Artikel 8 Absatz 2.

Absatz 7 dient der Umsetzung von Artikel 7 Absatz 2 der Richtlinie (EU) 2023/977.

Absatz 8

§ Absatz 8 Satz 1 bestimmt zunächst, dass eine Übermittlung personenbezogener Daten auch im Rahmen des Informationsaustausches im Anwendungsbereich der Richtlinie (EU) 2023/977 nur unter den Voraussetzungen des § 89 erfolgen darf. Zudem dient Absatz 8 Satz 1 mit seiner Beschränkung der Übermittlung personenbezogener Daten auf solche, die unter eine in Anhang II Abschnitt B der Europol-Verordnung fallen, der Umsetzung von Artikel 10 Buchstabe b der Richtlinie (EU) 2023/977.

Absatz 8 Satz 2 setzt Artikel 9 Absatz 2 der Richtlinie (EU) 2023/977 um. Als nach dieser Vorschrift unverzüglich einzuholende gerichtliche Erlaubnisse kommen im präventiv-polizeilichen Kontext vor allem Entscheidungen über eine Datennutzung nach § 57 Absatz 8 Satz 5, § 63 Abs. 5 Satz 2, § 65 Absatz 3 Satz 2 in Betracht.

Zu Nummer 34

§ 91

Absatz 2

Zweck der Neufassung ist es, durch die Aufzählung der Löschungstatbestände eine anwenderfreundliche Regelung zu gestalten, insbesondere aber die Datenschutzrechte der betroffenen Personen zu gewährleisten. Die klarstellenden Löschungstatbestände unter den Nummern 3 bis 7 (neu) wurden zur Gewährleistung der Anwenderfreundlichkeit aufgenommen.

Die Änderungen der Absätze 3 und 4 stellen redaktionelle Folgeänderungen dar.

Zu Nummer 35

§ 93

Die Änderungen in Absatz 1 Nummer 10 erfolgen zur Behebung eines redaktionellen Versehens.

Zu Nummer 36

§ 94

Mit den Änderungen und Ergänzungen werden die Kontrollpflichten der oder des Sächsischen Datenschutz- und Transparenzbeauftragten erweitert. Neu aufgenommen wurden die Befugnisse nach § 57a Absatz 1 Satz 4 und Absatz 2, § 58 (verdeckter Einsatz der automatisierten Kennzeichenerkennung), § 62a Absatz 5 und Absatz 6, § 62b Absatz 2 und die Quellen-TKÜ durch die allgemeine Verweisung auf § 66. Die Ersetzung des Begriffs „Informationssystem“ durch den Begriff „Dateisystem“ resultiert aus der Streichung der Legaldefinition der bisherigen Nummer 7 des § 4.

Zu Nummer 37

§ 97

Die Bezeichnung „Polizeiverwaltungsamt“ in Absatz 1 Nummer 3 wird durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Der aktuelle Name „Polizeiverwaltungsamt“ spiegelt die Vielfältigkeit seiner Aufgaben sowie den Anspruch von Moderne und Innovation nicht mehr wider. Das Voranschreiten der Digitalisierung und das damit verbundene Erfordernis, die Zukunftsfähigkeit der Polizei Sachsen sicherzustellen, setzt auch die Gewinnung und Bindung von geeignetem Personal in Konkurrenz mit der freien Wirtschaft oder anderen öffentlichen Arbeitgebern voraus.

Zu Nummer 38

§ 101

Die Bezeichnung „Polizeiverwaltungsamt“ in Absatz 1 wird durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Der aktuelle Name „Polizeiverwaltungsamt“ spiegelt die Vielfältigkeit seiner Aufgaben sowie den Anspruch von Moderne und Innovation nicht mehr wider. Das Voranschreiten der Digitalisierung und das damit verbundene Erfordernis, die Zukunftsfähigkeit der Polizei Sachsen sicherzustellen, setzt auch die Gewinnung und Bindung von geeignetem Personal in Konkurrenz mit der freien Wirtschaft oder anderen öffentlichen Arbeitgebern voraus.

Zu Nummer 39

§ 106

Die Änderungen stellen Folgeanpassungen in Hinblick auf die geänderten Vorschriften § 21 und § 61 dar.

Zu Nummer 40

§ 106a

Absatz 1

Mit der Aufnahme der Regelung werden Ordnungswidrigkeitentatbestände im Hinblick auf das Zuwiderhandeln gegen vollziehbare Maßnahmen nach den §§ 18, 19, 20, 21 Absatz 1 bestimmt. Im Sächsischen Polizeibehördengesetz besteht eine entsprechende Regelung in § 31.

Absatz 2

Die Regelung bestimmt die Höhe der Geldbuße.

Absatz 3

Die Regelung bestimmt gemäß § 36 Absatz 1 Nummer 1 Ordnungswidrigkeitengesetz, dass die zuständige Verwaltungsbehörde die Polizeidienststelle ist, die die Anordnung getroffen hat.

Zu Nummer 41

§ 107

Die Änderungen und Ergänzungen in Satz 1 erfolgen in Konsequenz von Änderungen bestehender berichtspflichtiger Befugnisregelungen (Änderungen bei § 21, § 59 außer Kraft getreten) und im Hinblick auf in das Sächsische Polizeivollzugsdienstgesetz neu aufgenommener Befugnisregelungen, für welche wegen der damit verbundenen erheblichen Eingriffe in Grundrechte eine Berichtspflicht gegenüber der Öffentlichkeit sowie dem Landtag besteht. Von der Berichtspflicht nunmehr umfasst ist der Einsatz von Bodycam in Wohnungen nach § 57 Absatz 4 Satz 2 und Absatz 5 Satz 2. Ebenfalls in die Berichtspflicht aufgenommen wurden die neu aufgenommen Befugnisregelungen gemäß § 57a Absatz 1 Satz 4 und Absatz 2, die in § 60 neu aufgenommene Befugnis zur Ausschreibung zur Ermittlungsanfrage, die Befugnis nach § 62a Absatz 5 und 6 (Einsatz selbstlernender künstlicher Intelligenz und Erstellung eines Verhaltensprofils), § 62b Absatz 2 (biometrischer Abgleich mit Daten aus dem Internet) und § 66 Absatz 2 (Quellen-TKÜ). Die vorgesehenen Änderungen und Ergänzungen tragen den Anforderungen des Bundesverfassungsgerichts an die gesetzgeberische Ausgestaltung von Berichtspflichten zur Gewährung von Transparenz und Kontrolle von heimlichen Befugnisregelungen Rechnung (Urteil BVerfG 2016, 1 BvR 966/09, Rz. 142).

Zu Nummer 42

§ 108

Die Streichung der Norm erfolgt in Hinblick darauf, dass die Befristung von Einzelvorschriften durch Außerkrafttreten nicht mehr zulässig ist (Siehe Handbuch der Rechtsförmlichkeit).

Zu Artikel 2 (Weitere Änderung des Sächsischen Polizeivollzugsdienstgesetzes)

Durch die Änderungsbefehle des Artikels 2 werden Regelungen des Sächsischen Polizeivollzugsdienstgesetzes geändert, die nur für einen befristeten Zeitraum gelten sollen. Die Regelung steht in Zusammenhang mit Artikel 16 Inkrafttreten.

Durch Nummer 1 wird die Regelung der Erweiterung des Einsatzes von Distanz-Elektroimpulsgeräten auf Polizeibedienstete, deren Einsatz nicht innerhalb einer Spezialeinheit erfolgt, gestrichen.

Durch die Nummern 2 und 3 wird die Regelung zur Ausweitung des Einsatzes der Bodycam auf Wohnungen und die im Kontext bestehenden ergänzenden Regelungen gestrichen.

Durch die Nummer 4 wird die Regelung zur Quellen-TKÜ und die im Kontext bestehenden Regelungen gestrichen.

Durch die Regelung in Artikel 16 ordnet der Gesetzgeber an, zu welchem Zeitpunkt die Regelungen des Artikel 2 jeweils in Kraft treten.

Zu Artikel 3 (Änderung des Sächsischen Polizeibehördengesetzes)

Zu Nummer 1

§ 23 Absatz 2

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

Zu Nummer 2

§ 30 Absatz 1

Mit den Änderungen werden die Vorgaben des Sächsischen Verfassungsgerichtshofs durch Urteil vom 25. Januar 2024, Vf. 91-II-19, umgesetzt. Das Gericht bemängelte hinsichtlich des bisherigen § 30 Absatz 1 Nummer 2 SächsPBG, dass diese Regelung keine hinreichend bestimmten und klaren Vorgaben bezüglich des Anlasses, des Zwecks und der Grenzen der Maßnahme enthalte. Es fehle außerdem an einem inneren Zusammenhang zwischen den erwarteten Gefahren für die geschützten Objekte und einer auf tatsächlichen Anhaltspunkten basierenden besonderen Gefährdungslage als Voraussetzung für die Videoüberwachung.

In Umsetzung der Entscheidung wurde – auch unter Praxisgesichtspunkten – der bisherige Regelungsinhalt der Nummer 2 in Nummer 1 neu und der bisherige der Nummer 1 in Nummer 2 neu übernommen und angepasst. Voraussetzung für die Videoüberwachung nach beiden Befugnisregelungen ist nunmehr jeweils das Vorliegen einer tatsachenbasierten Gefahrenlage. Die Videoüberwachung nach dieser Vorschrift knüpft sowohl in Nummer 1 als auch in Nummer 2 an die gemeindliche Aufgabe der Gefahrenabwehr der Ortspolizeibehörden an.

Besondere gemeindliche Polizeibehörden wie beispielsweise das Umweltamt, das Bauamt etc. sind im Hinblick auf ihre fachaufgabenspezifische Zuständigkeit für die Gefahrenabwehr nicht Normadressaten des § 30 Abs. 1. Soweit diese besonderen gemeindlichen (Polizei)Behörden eine Videografie ins Auge fassen, kann dies nicht auf die Rechtsgrundlage des Polizeibehördengesetzes gestützt werden.

Soweit es um die Gewährleistung der öffentlichen Sicherheit und Ordnung auf einem öffentlich zugänglichen Platz geht, handelt es sich um die Aufgabe der allgemeinen Gefahrenabwehr der Ortspolizeibehörde gem. § 2 Abs. 1, d. h. der allgemeinen Aufgabe, Gefahren für die öffentliche Sicherheit oder Ordnung abzuwehren. Im Rahmen dieser Aufgabe sind auch Vorbereitungen zu treffen, um künftige Gefahren abwehren zu können, vergleiche § 2 Abs. 1 S. 2. Im Rahmen dieser Aufgabe bildet § 30 als bereichsspezifische Norm im Polizeibehördengesetz die entsprechende Ermächtigungsgrundlage für eine Videografie im öffentlichen Raum.

Die Rechtsgrundlagen der behördlichen Videoüberwachung gemäß Nummer 1 und der nach § 13 Absatz 1 2. Alt. Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) (Hausrecht) haben unterschiedliche Zielrichtungen und überlappen sich nicht. Während die Videoüberwachung gemäß Nummer 1 dem Vollzug der gemeindlichen Aufgabe der Gefahrenabwehr als Ortspolizeibehörde dient, knüpft die Videoüberwachung gemäß § 13 Absatz 1 2. Alt. SächsDSDG demgegenüber allein an das Hausrecht an den eigenen Gebäuden an. Beide Regelungen stehen parallel nebeneinander, so dass auch im Hinblick auf die unterschiedlichen Zielrichtungen und Voraussetzungen keine Sperrwirkung besteht.

Nummer 1

Mit der Änderung des Wortlauts der Regelung wird nunmehr klar bestimmt, welche gefährdeten Objekte unter welchen Voraussetzungen zu welchem Zweck videoüberwacht werden dürfen.

In Nummer 1 werden die Anlagen und Einrichtungen, zu deren Schutz die Videoüberwachung erfolgen kann, wie folgt konkret bezeichnet: öffentliche Einrichtungen, öffentliche

Verkehrsmittel, Kulturgüter, Dienstgebäuden oder sonstige baulichen Anlagen öffentlicher Stellen.

Mit dem Begriff der „öffentlichen Einrichtung“ wird auf den im Kommunalrecht verwandten Begriff Bezug genommen. Unter einer öffentlichen Einrichtung wird allgemein eine Einrichtung der Gemeinde verstanden, die im öffentlichen Interesse unterhalten wird und durch einen gemeindlichen Widmungsakt der allgemeinen Benutzung durch Gemeindeangehörige sowie ortsansässige Vereinigungen zugänglich gemacht wird. Dem Begriff der öffentlichen Einrichtung unterfallen z.B. Rathäuser, Museen, Sportplätze, öffentliche Schwimmbäder, Kanalisation, Wertstoffhöfe, etc.

Dem Begriff „Öffentliche Verkehrsmittel“ unterfallen alle Transportmittel, die in den öffentlichen Personennahverkehr eingebunden sind und der öffentlichen Personenbeförderung dienen. Hierzu zählen alle zugelassenen Luft-, Land- und Wasserfahrzeuge.

„Kulturgüter“ sind beispielsweise historische Brunnenanlagen, archäologische Stätten, Skulpturen oder unter Denkmalschutz stehende Ruinen.

Voraussetzung für die Videoüberwachung der genannten Objekte ist, dass Tatsachen die Annahme rechtfertigen, dass im unmittelbaren Umfeld der genannten gefährdeten Objekte künftig Straftaten oder Ordnungswidrigkeiten begangen werden, durch die Personen oder bedeutende Sach- oder Vermögenswerte gefährdet werden. Die Regelung setzt somit das Vorliegen einer entsprechenden Tatsachenbasis voraus, die geeignet ist, die Prognose künftiger Gefahren für die Rechtsgüter von Leib oder Leben oder bedeutende Sach- oder Vermögenswerte zu begründen. Hierfür bedarf es eines Lagebildes, dem Erkenntnisse zu künftigen Straftaten und Ordnungswidrigkeiten im Hinblick auf die Rechtsgüter „Leib“ oder „bedeutende Sach- oder Vermögenswerte“ entnommen werden können.

Nummer 2

Die bisherige Regelung in § 30 Absatz 1 Nummer 1 wurde mit Änderungen in die Nummer 2 überführt.

Unter dem Begriff „öffentlich zugänglichen Bereiche“ sind in Übereinstimmung mit den Begrifflichkeiten in § 57 SächsPVDG Bereiche zu verstehen, die zur öffentlichen Nutzung bestimmt sind. Ein solcher öffentlich zugänglicher Bereich kann innerhalb oder außerhalb eines Gebäudes liegen und ist nicht an das Vorhandensein eines Gebäudes geknüpft. Die Zweckbestimmung folgt aus einer entsprechenden förmlichen Widmung durch den Berechtigten oder dadurch, dass dieser in anderer Weise seinen Willen deutlich macht, dass eine solche öffentliche Zugänglichkeit bestehen soll. Beispielsweise fallen dem allgemeinen Verkehr förmlich gewidmete öffentliche Straßen, Wege und Plätze unter diesen Begriff. Entscheidend ist die durch den Berechtigten eröffnete tatsächliche Nutzungsmöglichkeit durch die Allgemeinheit.

Voraussetzung für eine Videoüberwachung nach Nummer 2 ist eine tatsachenbasierte Gefahrenlage, die die Annahme rechtfertigt, dass dort erhebliche Gefahren für die öffentliche Sicherheit entstehen.

Die Klarstellung der Erforderlichkeit der Maßnahme durch die Regelung im 2. Halbsatz soll verdeutlichen, dass die Videoüberwachung auch in räumlicher oder zeitlicher Hinsicht zur Gefahrenabwehr erforderlich sein muss.

Zu Nummer 3

§ 40 Absatz 1

Mit den Änderungen und Ergänzungen erfolgen die erforderlichen Anpassungen an die Änderungen der datenschutzrechtlichen Bestimmungen des Sächsischen Polizeivollzugsdienstgesetzes. Der bisherige Regelungsinhalt von § 80 Absatz 1 und 7 wurde in § 79 Absatz 1 und 2 und der bisherige Regelungsinhalt von § 79 wurde in § 79a übernommen. Die Einschränkung in der Verweisung auf § 79a erfolgt vor dem Hintergrund, dass die Absätze 3, 4 und 6 allein an den Polizeivollzugsdienst adressiert sind. Vor dem Hintergrund der Ergänzung von § 84 Absatz 3 um Befugnisregelungen zur Datenübermittlung an nichtöffentliche Stellen im Kontext von „häuslicher Gewalt“ (Nummern 4 und 5 neu) bestand das Erfordernis, diese Befugnisregelung von der Anwendbarkeit auszuschließen, da diese Aufgabe allein dem Polizeivollzugsdienst obliegt. Ferner wurde die neue Regelung des § 89a SächsPVDG ausgeschlossen, da auch diese allein für den Polizeivollzugsdienst Anwendung findet.

Zu Nummer 4

§ 42

Mit der Änderung in Satz 1 erfolgt die Korrektur eines redaktionellen Versehens analog zu der Änderung in § 48 Absatz 3 Satz 1 SächsPVDG.

Zu Artikel 4 (Einschränkung von Grundrechten)

Artikel 3 wurde neu eingefügt, um dem Zitiergebot Rechnung zu tragen. Die Aufnahme der Regelung wurde aufgrund des Umstands, dass das Gesetz zur Änderung polizeirechtlicher Vorschriften selbst Grundrechtseinschränkungen enthält oder bereits bestehende Grundrechtseinschränkungen erweitert, notwendig.

Zu Artikel 5 (Änderung des Sächsischen Kontrollgesetzes)

Die Streichung von § 59 folgt in Konsequenz des Außerkrafttretens der Regelung durch Zeitablauf zum 31. Dezember 2023 (siehe bisherige Regelung in § 108 Absatz 1). Mit den Änderungen wird die Kontrollbefugnis des Parlamentarischen Kontrollgremiums auf die neuen eingriffsintensiven und heimlichen Befugnisse gemäß § 60 Absatz 1 (Ausschreibung zur gezielten Befragung) und § 66 Absatz 2 (Quellen-TKÜ) erweitert.

Zusammen mit der Erweiterung der Berichtspflichten an die Sächsische Datenschutz- und Transparenzbeauftragte in § 94 und an die Öffentlichkeit und das Parlament in § 107 wird den Anforderungen des Bundesverfassungsgerichts im Urteil vom 20. April 2016, 1 BvR 966/09, Rz. 141 und 142 nachgekommen und sowohl eine effektive aufsichtliche Kontrolle als auch die erforderliche Transparenz polizeilichen Handelns gewährleistet.

Zu Artikel 6 (Änderung des Sächsischen Gesetzes zur Regelung polizeilicher Zuverlässigkeitsüberprüfungen)

§ 4 Satz 3 Nummer 4

Ziel der Änderung ist die Parallelgestaltung der Regelung zur Anfrage bei den zuständigen Polizeien analog zu der Regelung in § 88. Durch die Prüfstellen der Polizei wird darauf hingewiesen, dass insbesondere ein erheblicher Teil der eingesetzten Handwerker ausländische Personen sind, die teils einen festen Wohnsitz in Deutschland haben, teils aber auch nicht. Diese Situation birgt aus Sicht der Prüfstellen eine erhebliche Sicherheitslücke. Insbesondere angesichts der sich zuspitzenden weltweiten Konflikte wird die Gefahr gesehen, dass sächsische Polizeidienststellen aufgrund der fehlenden Informationsgewinnung Opfer von Straftaten werden könnten.

§ 4 Satz 3 Nummer 5

Ziel der Änderung ist die Parallelgestaltung der Regelung zur Anfrage bei dem Landesamt für Verfassungsschutz analog zu der Regelung in § 88 für den Fall, dass im Einzelfall eine Anfrage erforderlich ist.

Zu Artikel 7 (Folgeänderung im Sächsischen Besoldungsgesetz)

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in der Anlage 2 (zu § 24 Absatz 1) durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 8 (Folgeänderung im Sächsischen Verwaltungsorganisationsgesetz)

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 8 Absatz 1 Nummer 4 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 9 (Folgeänderung im Sächsischen Personalvertretungsgesetz)

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 68 Absatz 1 Nummer 4 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 10 (Folgeänderungen im Sächsischen Straßenverkehrsrechtsgesetz)

Zu Nummer 1

§ 14

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 14 Absatz 1 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Nummer 2

§ 18

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 18 Absatz 2 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 11 (Folgeänderungen in der Sächsischen Polizeiorganisationsverordnung)

Zu Nummer 1

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in der Inhaltsübersicht zu § 4, § 1 Absatz 1, § 4 Absatz 1, § 4 Absatz 2, § 4 Absatz 3 Satz 1 und 2 und § 4 Absatz 4 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Nummer 2

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in der Inhaltsübersicht zu § 4, § 1 Absatz 1, § 4 Absatz 1, § 4 Absatz 2, § 4 Absatz 3 Satz 1 und 2 und § 4 Absatz 4 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 12 (Folgeänderung in der Sächsischen Waffengesetzdurchführungsverordnung)

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 2 Absatz 1 Nummer 2 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG

Zu Artikel 13 (Folgeänderung in der Sächsischen Vertretungsordnung)

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 6 Absatz 3 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 14 (Folgeänderung in der Sächsischen Heilfürsorgeverordnung)

Zu Nummer 1

§ 2 Absatz 7

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 2 Absatz 7 Satz 2 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Nummer 2

§ 30

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 30 jeweils durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 15 (Folgeänderungen in der Sächsischen Straßenverkehrsrechtsverordnung)

Zu Nummer 1

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 5 jeweils durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Nummer 2

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 9 Absatz 2 Satz 2 jeweils durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 16 (Inkrafttreten)

Die Regelung enthält die Bestimmung zum Inkrafttreten dieses Mantelgesetzes.

Absatz 1 bestimmt das grundsätzliche Inkrafttreten für den Tag nach der Verkündung. Die Absätze 2 bis 4 enthalten hiervon abweichende Bestimmungen.

Absatz 2 regelt für das Inkrafttreten des Einsatzes von Distanz- Elektroimpulsgeräten abweichend die Frist 1. Januar 2027. Dadurch wird berücksichtigt, dass der Polizeivollzugsdienst ausreichend Zeit für Schulungsmaßnahmen benötigt. Für die Spezialeinheiten gilt die bisherige Regelung bis zur Inkraftsetzung der neuen Regelung weiter.

Absatz 3 bestimmt, dass die Erweiterung des Einsatzes der Bodycam in Wohnungen und die begleitenden gesetzlichen Folgeanpassungen sowie die Regelungen zur Quellen-TKÜ und die begleitenden gesetzlichen Folgeanpassungen zum 31. Dezember 2031 außer Kraft treten.

Absatz 4 bestimmt für die Regelung der Erweiterung des Einsatzes von Distanz- Elektroimpulsgeräten die Geltungsdauer bis zum 31. Dezember 2032.



Sächsischer
Städte- und
Gemeindetag

Sächsischer Städte- und Gemeindetag e.V.
Glacisstraße 3, 01099 Dresden

nur per E-Mail: Anhoerung.SaechsPVDG@smi.sachsen.de

Sächsisches Staatsministerium des Innern
Stellvertretende Referatsleiterin Recht der Polizei
Frau Peggy Frey
Wilhelm-Buck-Str. 2
01097 Dresden

Ihre Nachricht vom	Ihr Zeichen	Unser Zeichen	Bearbeiter	Az. / ID-Nr.	Telefon	Datum
06.10.2025	36-2002/ 25/14	Se/CF	Frau Seubert	100.00 / 230187	-130	17.11.2025

Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG); Anhörung des Referentenentwurfes

Sehr geehrte Frau Frey,

für die Gelegenheit zur Stellungnahme in vorbezeichneter
Angelegenheit danken wir Ihnen.

Artikel 1 Änderung des SächsPVDG

Es liegt zwar keine direkte kommunale Betroffenheit bezüglich der geplanten Novellierung vor, dennoch befürworten wir grundsätzlich die geplanten Neuregelungen. Denn mit den neuen polizeilichen Befugnissen wird auch das Sicherheitsbedürfnis in den Kommunen gestärkt.

Zudem setzt der Entwurf Vorgaben des Sächsischen Verfassungsgerichtshofs um und erfüllt teilweise Vorhaben aus dem Koalitionsvertrag. Auch die geänderte Sicherheitslage erfordert zudem eine Anpassung der polizeilichen Befugnisse, auf die wir nachfolgend noch näher eingehen.

Zu § 18 SächsPVDG

Wir befürworten die Erweiterung bzw. Wiederaufnahme des Tatbestandsmerkmals der „öffentlichen Ordnung“ in § 18 SächsPVDG zur Platzverweisung (wie es in § 21 Abs. 1 SächsPolG a. F. bereits enthalten war).

Sächsischer Städte- und
Gemeindetag e.V.

Glacisstraße 3
01099 Dresden
Telefon 0351 8192-0

Internet:
<http://www.ssg-sachsen.de>

E-Mail:
post@ssg-sachsen.de

Steuernummer: 202/141/03088

So erreichen Sie uns:
Straßenbahnlinien
3, 7, 8
Haltestelle Carolaplatz,
6, 13 Haltestelle
Rosa-Luxemburg-Platz
oder per Bahn
Bahnhof Dresden-Neustadt

Begründung:

Nach § 21 Abs. 1 SächsPolG a. F. konnte die Polizei zur Abwehr einer Gefahr für die öffentliche Sicherheit oder Ordnung oder zur Beseitigung einer Störung eine Person vorübergehend von einem Ort verweisen oder ihr vorübergehend das Betreten eines Ortes verbieten.

Da nach § 2 Abs. 1 S. 1 SächsPVDG die Polizei die Aufgabe hat, Gefahren für die öffentliche Sicherheit oder Ordnung abzuwehren (Gefahrenabwehr), ist eine gleichlautende Formulierung in § 18 SächsPVDG erforderlich.

Artikel 2 Änderung des Sächsischen Polizeibehördengesetz (SächsPBG)

Zu § 23 Absatz 2 SächsPBG

Im neugefassten § 23 Absatz 2 SächsPBG ist anstatt auf § 23 Absatz 1 Satz 1 Nummer 2 SächsPBG auf § 23 Absatz 1 Satz 1 Nummer 1 SächsPBG zu verweisen.

Begründung:

Mit der Änderung sollte eine zu § 29 Abs. 3 SächsPVGD analoge Änderung erfolgen. Der Ausnahmetatbestand bezieht sich auf die in § 29 Abs. 1 Satz 1 Nummer 2 des SächsPVDG genannten Gefahr für Leib, Leben, Freiheit einer Person oder bedeutende Sach- und Vermögenswerte. Die analoge Regelung dazu befindet sich jedoch in § 23 Abs. 1 Satz 1 Nummer 1 SächsPBG und nicht in § 23 Absatz 1 Satz 1 Nummer 2 SächsPBG. Demzufolge sollte der Bezug in § 23 Abs. 2 SächsPBG auf Nummer 1 geändert werden.

Zur Gesetzesbegründung zu § 23 Absatz 2 SächsPBG

In der Gesetzesbegründung zu § 23 Absatz 2 SächsPBG muss der Verweis auf die Streichung des bisherigen Satz 3 in § 23 Absatz 2 SächsPBG entfallen.

Begründung:

§ 23 Absatz 2 SächsPBG in der bisherigen Fassung enthält keinen Satz 3.

Zu 30 Abs. 1 Nr. 2 SächsPBG

Die bisherige Regelung in § 30 Absatz 1 Nummer 1 SächsPBG wurde mit Änderungen in die Nummer 2 überführt.

§ 30 Abs. 1 Nr.1 SächsPBG sollte nach unserer Ansicht aber in seiner gegenwärtigen Fassung in die Nummer 2 überführt werden.

Begründung:

Denn es ist unklar, worauf sich der neue Begriff „sonstige erhebliche Gefahren für die öffentliche Sicherheit" bezieht, da bislang erhebliche Gefahren für die öffentliche Sicherheit ausreichen.

Unklar ist auch, aus welchen Gründen nicht mehr der Begriff der „öffentlich zugänglichen Räume" verwendet wird, sondern nunmehr der Begriff des „öffentlich zugänglichen Bereiches" und ob dies einen Unterschied bedingt oder nicht.

Der Sächsische Verfassungsgerichtshof hat § 30 Abs. 1 Nr. 1 SächsPBG in seiner gegenwärtigen Fassung für mit der Verfassung vereinbar erklärt. Daher sollte diese Regelung in ihrer gegenwärtigen Fassung auch künftig so belassen werden um Unklarheiten in der Rechtsanwendung zu vermeiden.

Soweit Sie um Stellungnahme baten, welche weiteren, im Entwurf nicht enthaltenen Eingriffsbefugnisse polizeifachlich für erforderlich halten, möchten wir folgt ausführen:

Regelung der Befugnis zur Gewahrsamnahme für die Polizeibehörden (vgl. § 22 SächsPVDG)

Bislang enthält das Sächsische Polizeibehördengesetz keine Regelung/Befugnis zur Gewahrsamnahme analog zu § 22 SächsPVDG. Eine solche Befugnis sollte auch in das Sächsische Polizeibehördengesetz aufgenommen werden.

Begründung:

Eine Gewahrsamnahme ist insbesondere dann von Relevanz, wenn sich beispielsweise aufgrund einer Identitätsfeststellung (IDF) ergibt, dass die Person von der Polizei gesucht wird (z. B. offene Aufenthaltsermittlungen, Vermögensabschöpfungen, offene Haftbefehle), allerdings die IDF bereits beendet ist, ohne dass die Polizei bereits vor Ort eingetroffen ist. Die gesuchte Person müsste dann nach dem Willen des Gesetzgebers aus der Maßnahme entlassen werden, da keine Rechtsgrundlage für das weitere Festhalten ersichtlich ist. Vielfach wird der gemeindliche Vollzugsdienst in derartigen Fällen durch den Polizeivollzugsdienst gebeten, die Person zur Dienststelle der Polizei (z. B. mit einem Dienstfahrzeug der Kommune) zu verbringen. Auch insoweit fehlt es aber an einer entsprechenden Rechtsgrundlage/Befugnis. Gleiches gilt für die Befugnis zu einem Zuführungsgewahrsam von Minderjährigen (vgl. § 22 Abs. 2 SächsPVDG) beispielsweise nach durchgeführten Jugendschutzkontrollen oder im Zusammenhang mit dem Thema „Schulverweigerer".

Regelung der Befugnis zur Durchsuchung zur Eigensicherung für die Polizeibehörden (vgl. § 27 Abs. 2 SächsPVDG)

Die Regelung des § 27 Abs. 2 SächsPVDG sollte in das SächsPBG übernommen werden.

Begründung:

In der Praxis zeigt sich, dass im Einzelfall Durchsuchungen bereits beim Ergreifen aggressiver Personen zur Eigensicherung notwendig sind, um eventuelle Überraschungsangriffe zu verhindern.

Rechtsgrundlage zur Nutzung von Bodycams für die Polizeibehörden (vgl. § 57 SächsPVDG)

Es sollte auch im Sächsischen Polizeibehördengesetz eine Rechtsgrundlage zur Nutzung von Bodycams geschaffen werden.

Begründung:

Vielfach sind die kommunalen Polizeibehörden als erste vor Ort und insoweit könnten sie bereits deeskalierend agieren.

Darüber hinaus gibt es regelmäßig Übergriffe auf kommunale Polizeibehörden (z. B. Widerstandshandlungen, Beleidigungen oder Bedrohungen). Es ist daher kein Grund ersichtlich, weshalb die kommunalen Polizeibehörden weniger schützenswert seien als der Polizeivollzugsdienst. Dies insbesondere auch vor dem Hintergrund, dass die kommunalen Polizeibehörden im Rahmen der Anwendung des unmittelbaren Zwangs nur bestimmte Hilfsmittel der körperlichen Gewalt sowie als Waffe den Schlagstock einsetzen dürfen. Der Einsatz von Bodycams wird daher sowohl präventiv als auch im Nachgang zur Dokumentation von Einsätzen als zweckmäßig angesehen.

Schaffung einer Regelung für Zufahrtssperren bei Veranstaltungen

Wir fordern eine gesetzliche Klarstellung in § 2 Abs. 1 S. 3 SächsPVGD, dass die Terrorabwehr im Zusammenhang mit der Sicherheit von öffentlichen Veranstaltungen als vorbeugende Bekämpfung von Straftaten eine Aufgabe des Polizeivollzugsdienstes ist und die Kosten für diese vorbeugende Bekämpfung von Straftaten vom Freistaat Sachsen getragen werden.

Begründung:

Unser Präsidium hat in seiner Sitzung am 27. August 2025 den vorgenannten Regelungsvorschlag beschlossen.

Dazu gibt es folgenden Hintergrund:

Infolge der Terroranschläge u. a. in Magdeburg, Mannheim und München sind die Anforderungen der Polizei an die Sicherheitskonzepte u. a. von Weihnachtsmärkten deutlich gestiegen. Das stellt die Kommunen und Veranstalter nicht nur in Sachsen, sondern bundesweit vor ganz erhebliche Herausforderungen. Maßgeblich für die konkreten Sicherungsmaßnahmen beispielsweise durch Zufahrtsschutzelemente ist die Beurteilung der jeweiligen örtlichen abstrakten Gefährdungslage durch die Polizei.

Die Polizei geht derzeit von einer hohen abstrakten Gefährdungslage aus und fordert für öffentliche Veranstaltungen ein Sicherheitskonzept mit einem Zufahrtsschutz.

Grundlage der polizeilichen Beratung zu erforderlichen Sicherheitsmaßnahmen sind eine aktuelle Gefährdungslagebewertung und die Betrachtung individueller Rahmenbedingungen der konkreten Veranstaltung.

Die Umsetzung der Sicherheitsmaßnahmen obliegt grundsätzlich dem Veranstalter im Rahmen behördlicher Auflagen. Diese sind verbindlich und Teil des kooperativen, abgestimmten Sicherheitskonzepts.

Zu beachten ist in diesem Zusammenhang auch, dass es in Sachsen bislang keine Anzeige- und Genehmigungspflicht für öffentliche Veranstaltungen gibt.

Fazit:

Letztlich ist die Situation für die Veranstalter von Weihnachtsmärkten u. a. öffentlichen Veranstaltungen abhängig von der Beurteilung der jeweiligen örtlichen abstrakten Gefährdungslage durch die Polizei.

Das bedeutet, dass die Polizei Vorgaben zum Zufahrtsschutz im Rahmen der Gefahrenprognose gegenüber den Kommunen macht, die über die finanzielle Leistungsfähigkeit der Kommunen hinaus gehen, ohne dass sich die Polizei an diesen Kosten beteiligt. Unser Nachbarbundesland erkennt demgegenüber die Notwendigkeit einer Kostenbeteiligung des Freistaates bereits an und stellt ein Budget von 5 Mio. Euro zur Verfügung.

Allein Leipzig und Dresden müssen in diesem Jahr jeweils fast zwei Millionen Euro zusätzlich für Sicherheitsvorkehrungen ausgeben.

Aktuell hat auch der Deutsche Städtetag den Bund und die Länder aufgefordert, sich an den Kosten für die Sicherheit auf den Weihnachtsmärkten zu beteiligen.

Der Grundsatz „Wer bestellt, bezahlt“ wird somit seitens des Landes durch die Vorgaben der Polizei für einen Zufahrtsschutz für öffentliche Veranstaltungen konterkariert.

Rechtliche Bewertung:

Nach Art. 73 Abs. 1 Nr. 9a Grundgesetz hat der Bund die ausschließliche Gesetzgebung für die Abwehr von Gefahren des internationalen Terrorismus in den Fällen, in denen eine länderübergreifende Gefahr vorliegt, die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder die oberste Landesbehörde um eine Übernahme ersucht.

Folglich besteht grundsätzlich eine vorrangige Zuständigkeit der Landespolizei für die Terrorabwehr.

Auch nach § 2 Abs. 1 S. 3 SächsPVDG und nach § 4 Abs. 1 S. 2 SächsPBG ist ausschließlich die (staatliche) Polizei (Polizeivollzugsdienst) für die vorbeugende Bekämpfung von Straftaten zuständig.

Der Zufahrtsschutz bei öffentlichen Veranstaltungen gehört zur vorbeugenden Bekämpfung von Straftaten.

Die vorbeugende Bekämpfung von Straftaten ist aber eine Aufgabe des Polizeivollzugsdienstes sowie des Staates und nicht der kommunalen Polizeibehörden. Folglich muss der Freistaat Sachsen auch die Kosten tragen, die für diese vorbeugende Bekämpfung von Straftaten entstehen.

Es liegt auch keine Gefahrenvorsorge nach § 2 Abs. 1 Satz 2 des SächsPBG vor, weil die Gefahrenvorsorge eine Gefahr voraus. Eine Gefahr im polizeirechtlichen Sinne liegt vor, wenn die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für die öffentliche Sicherheit eintritt. Daran fehlt es aber in den Fällen des Zufahrtsschutzes bei öffentlichen Veranstaltungen, weil die vorgenannte hinreichende Wahrscheinlichkeit eines absehbaren Schadens für die öffentliche Sicherheit fehlt, da nur eine generell-abstrakte Gefahr aus Sicht der Polizei vorliegt.

Koalitionsvertrag:

Der aktuelle Koalitionsvertrag zwischen CDU und SPD führt aus, dass für die Sicherheit u. a. von öffentlichen Veranstaltungen und Einrichtungen in Abstimmung mit den Kommunen das Sächsische Polizeibehördengesetz fortgeschrieben werden soll. Dazu sollen laut Koalitionsvertrag Verfahren und Zuständigkeiten präzisiert und praktikable Lösungen für aktuelle Bedrohungsszenarien erarbeitet werden. Bislang gibt es dazu keine Gesetzesentwürfe.

Wir fordern daher, dass bereits im jetzigen Gesetzgebungsverfahren eine Regelung für die Zufahrtssperren bei Veranstaltungen erfolgt und die Kommunen nicht auf ein eventuelles zukünftiges separates Gesetzgebungsverfahren zum Polizeibehördengesetz vertröstet werden.

Abschließend weisen wir darauf hin, dass diese Stellungnahme unter Gremienvorbehalt steht. Sofern im Rahmen der Beschlussfassung in unserem Landesvorstand am 12. Dezember 2025 Änderungen bzw. Ergänzungen erforderlich sein sollten, werden wir Sie umgehend informieren.

Wir bitten nun um Berücksichtigung unserer Anmerkungen im weiteren Verfahren und stehen für weitere Rückfragen gern zur Verfügung.

Mit freundlichen Grüßen



Mischa Woitscheck
Geschäftsführer

Sächsischer Landkreistag • Käthe-Kollwitz-Ufer 88 • 01309 Dresden

Sächsisches Staatsministerium des Innern
Referat 36 – Recht der Polizei
Frau stv. Referatsleiterin
Peggy Frey
Wilhelm-Buck-Straße 2
01097 Dresden

Bearbeiter Herr Lange
Telefon 0351 31801-29
Telefax 0351 31801-44
E-Mail slkt@lkt-sachsen.de
Internet www.lkt-sachsen.de

Az. 104.20 / 253902 / Lan

Datum 23.11.2025

Nur per E-Mail an: Anhoerung.SaechsPVDG@smi.sachsen.de

Novellierung des Polizeivollzugsdienstgesetzes (SächsPVDG)

Stellungnahme des Sächsischen Landkreistages

Sehr geehrte Frau Frey,

wir danken Ihnen herzlich für die Gelegenheit im Rahmen der Anhörung zur Novellierung des Polizeivollzugsdienstgesetzes (SächsPVDG) Stellung nehmen zu können.

Der Sächsische Landkreistag begrüßt den Gesetzentwurf.

Die sächsische Polizei muss auch aus unserer Sicht diejenigen Kompetenzen erhalten, die benötigt werden, um unsere Bevölkerung vor kriminellen Akten wirksam schützen zu können. Der vorliegende Gesetzentwurf entspricht dieser Zielstellung und gewährleistet polizeiliche Kompetenzen auf der Höhe der Zeit und im Einklang mit den Landespolizeigesetzen in anderen Bundesländern.

Dies betrifft ausdrücklich die Kernpunkte des Novellierungsvorhabens:

- § 12a SächsPVDG: Neue Befugnisse zur Drohnenabwehr mit technischen Geräten wie Laser und Störsender
- § 40 SächsPVDG: Einsatz von Tasern (Distanz-Elektroimpulsgeräten)
- § 57 SächsPVDG: Erweiterung des Einsatzes von Bodycams in öffentlich zugänglichen Bereichen auf den Bereich von Wohnungen und Geschäftsräume außerhalb der Öffnungszeiten
- § 57a SächsPVDG: KI-gesteuerte Datenanalyse
- § 58 SächsPVDG: Regelung zur automatisierten Kennzeichenerkennung
- § 62a SächsPVDG: Automatisierte Datenanalyse

- § 62b SächsPVDG: Anlassbezogener Abgleich mit öffentlich zugänglichen Internetdaten
- § 66 SächsPVDG: Quellen-Telekommunikationsüberwachung

Daneben setzt der Gesetzentwurf die in den letzten Jahren ergangene verfassungsgerichtliche Rechtsprechung um, die das Spannungsfeld von der Stärkung der öffentlichen Sicherheit und den Eingriffen in Grundrechte abbildete, in dem sich das Polizeirecht stets befindet. Hervorzuheben ist die umfassende Befassung Ihres Staatsministeriums mit diesen Rechtsprechungen. In den Begründungen zu vielen Neuregelungsvorhaben ist umfassend erläutert, inwiefern die Rechtsprechungen des Bundesverfassungsgerichtes und des Sächsischen Verfassungsgerichtshofes beachtet und in die neuen Regelungen implementiert worden sind. Es ist zu spüren, dass das SMI und die sächsische Staatsregierung an diesen Stellen das Ziel verfolgt haben sehr präzise zu arbeiten um eine erneute Verfassungswidrigkeit dieser Regelungen auszuschließen.

Aus kommunaler Sicht besteht kaum eine direkte Betroffenheit über diesen Gesetzentwurf. Eine kommunale Betroffenheit entsteht nur an den unter Punkt 2 zu Artikel 2 genannten Änderungen des Sächsischen Polizeibehördengesetzes. Hier erfolgt eine Abänderung von Eingriffsschwellen durch die vorgegebene verfassungsrechtliche Rechtsprechung. Sachlich zuständig für diese Maßnahmen sind gemäß § 6 Abs. 1 SächsPBG die Gemeinden als Ortspolizeibehörden.

Wir bitten daher um Verständnis, dass wir von einer Antwort zu den im Anschreiben aufgeworfenen polizeifachlichen Fragen absehen.

Mit freundlichen Grüßen



Jacob



Die Sächsischen
Industrie- und Handelskammern

IHK Chemnitz / Postfach 4 64 / 09004 Chemnitz

Sächsisches Staatsministerium des Inneren
z.Hd. Frau Peggy Frey
Wilhelm-Buck-Str. 2
01097 Dresden

Ihr Zeichen/Ihre Nachricht:

Ihr Ansprechpartner:
Herr Kristian Henschel

Telefon: 0371 6900-1101

E-Mail: kristian.henschel@chemnitz.ihk.de

Internet: ihk.de/chemnitz

Chemnitz, 10.11.2025

Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG) Anhörung zum Referentenentwurf

Sehr geehrte Frau Frey,

in oben genannter Angelegenheit bedanken wir uns im Namen der sächsischen Industrie- und Handelskammern für die Möglichkeit zur Stellungnahme zur Novellierung des Sächsischen Polizeivollzugsdienstgesetzes.

Die Sicherheit ist ein elementarer Wirtschaftsfaktor für unsere Mitgliedsunternehmen. Insoweit ist eine Anpassung an aktuelle Entwicklungen grundsätzlich im Interesse der Wirtschaft zu begrüßen. Ungeachtet technischer Neuerungen müssen indes auch die personellen Ressourcen von Polizei und Ordnungskräften auf ein adäquates Maß angepasst werden, um neben den Herausforderungen der Cyberkriminalität auch auf klassische Eigentumsdelikte, insbesondere im Einzelhandel, abschreckend reagieren zu können. Die konkreten Gesetzesänderungen haben indes aus unserer Sicht allenfalls einen mittelbaren Bezug zu unseren Mitgliedsunternehmen. Aus diesem Grunde sehen wir von einer weiteren Stellungnahme zu der geplanten Novellierung ab.

Im Namen der Landesarbeitsgemeinschaft
der sächsischen Industrie- und Handelskammern

Christoph Neuberg
Hauptgeschäftsführer der IHK Chemnitz

Landesarbeitsgemeinschaft
der Industrie- und Handelskammern
im Freistaat Sachsen

IHK Chemnitz
Straße der Nationen 25
09111 Chemnitz
Telefon +49 371 6900-0
Telefax +49 371 6900-191565
chemnitz@chemnitz.ihk.de
www.chemnitz.ihk24.de

IHK Dresden
Langer Weg 4
01239 Dresden
Telefon +49 351 2802-0
Telefax +49 351 2802-280
service@dresden.ihk.de
www.dresden.ihk.de

IHK zu Leipzig
Goerdelerring 5
04109 Leipzig
Telefon +49 341 1267-0
Telefax +49 341 1267-1421
info@leipzig.ihk.de
www.leipzig.ihk.de



**Bund Deutscher
Kriminalbeamter
Sachsen**

BDK Sachsen | Großenhainer Str. 237 | D-01129 Dresden

Sächsisches Staatsministerium des Innern

per Mail an

Polizeirecht@smi.sachsen.de

Landesgeschäftsstelle

Ansprechpartner/in: Torsten Schmorte
Funktion: Landesvorsitzender

E-Mail: lv.sachsen@bdk.de
Telefon: +49 351 496 1001

Datum: 13.11.2025

Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG);

Beteiligung nach § 119 des Sächsischen Beamtengesetzes

Stellungnahme Bund Deutscher Kriminalbeamter Landesverband Sachsen e.V.

*Schreiben des Sächsischen Staatsministeriums des Innern vom 6. Oktober 2025,
Az.: 36 -2002/25/14*

Sehr geehrte Damen und Herren,

der Bund Deutscher Kriminalbeamter – Landesverband Sachsen bedankt sich für die Möglichkeit, zum Referentenentwurf des novellierten Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG) Stellung zu nehmen.

Wir erkennen den klaren Willen des Gesetzgebers an, das Polizeirecht des Freistaates Sachsen auf ein modernes, technologisch zeitgemäßes und verfassungsrechtlich abgesichertes Fundament zu stellen. Die Umsetzung aktueller Rechtsprechung, insbesondere der gestuften Gefahrenbegrifflichkeit und neuer technischer Befugnisse, ist grundsätzlich zu begrüßen. Der Entwurf sieht eine substanzielle Modernisierung vor, die es ermöglicht, auf Bedrohungslagen wie Terrorismus, gewalttätigen Extremismus und hybride Angriffe flexibel zu reagieren. Vorratsbefugnisse im Bereich Observation, verdeckte Ermittlungen, TASER sowie Bodycams auch in Wohnungen gehen über die vorherigen Möglichkeiten hinaus und stärken die Handlungsfähigkeit der Polizei bei akuter Gefahr. Insbesondere die umfassende Videoüberwachung an Kriminalitätsschwerpunkten sowie Drohnen- und KI-basierte Echtzeiterkennung schaffen innovative Schutzmechanismen für polizeiliche Einsatzlagen. Ein zentrales Anliegen des Bundes Deutscher Kriminalbeamter ist, dass

spezielle polizeiliche Erhebungs- und Eingriffsnormen wie Observation, Quellen-TKÜ und verdeckte Ermittlungen, KI-Anwendungen auf realistische Schwellenwerte abstellen. Wird der Tatverdacht zu hoch angesetzt, sind die Normen praktisch wertlos, da in einer Vielzahl der Fälle bereits staatsanwaltschaftliche Ermittlungen laufen würden.

Gleichwohl sehen wir an mehreren Stellen erheblichen Anpassungsbedarf, um die Praxistauglichkeit und Systemkohärenz des Gesetzes sicherzustellen. Im Folgenden fassen wir die wesentlichen Punkte unserer Bewertung zusammen:

1. Fehlende Befugnis zur Prüfspeicherfrist (§§ 80 ff. SächsPVDG-E)

Der Referentenentwurf des Gesetzes zur Änderung polizeirechtlicher Vorschriften des Freistaates Sachsen regelt umfassend die Befugnisse der Polizei zur Datenerfassung und -speicherung. Dabei berücksichtigt der Entwurf die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) und des Sächsischen Verfassungsgerichtshofs (SächsVerfGH).

Ein zentrales Element ist die Regelung der vorsorgenden Speicherung personenbezogener Daten in § 80 ff. SächsPVDG-E. Diese Norm unterscheidet nach Personenkategorien (Verurteilte, Beschuldigte, Verdächtige, Anlasspersonen) und verknüpft jede Speicherung mit einer Negativprognose: Die Polizei darf Daten nur speichern, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Person künftig Straftaten begehen wird. Diese Grundkonzeption ist verfassungsrechtlich solide. Allerdings sieht der Entwurf keine Prüfspeicherfrist vor, obwohl das Bundesverfassungsgericht (Urt. v. 01.10.2024 – 1 BvR 1160/19) ausdrücklich betont hat, dass eine vorübergehende Speicherung zur Prüfung der Relevanz personenbezogener Daten sowohl zulässig als auch verfassungsrechtlich geboten ist. Der Entwurf verlangt implizit, dass die Negativprognose bereits bei der Ersterfassung der Daten vollständig vorliegen muss. § 80 Abs. 1 Nr. 4 SächsPVDG-E (Anlasspersonen) beispielsweise verlangt: „tatsächliche Anhaltspunkte dafür, dass [die Person] künftig Straftaten von erheblicher Bedeutung begehen wird“. Dies bedeutet in der Praxis: Ohne diese tatsächlichen Anhaltspunkte darf die Polizei die Daten nicht speichern – selbst wenn sie für künftige Gefahrenabwehr relevant sein könnten.

Die praktische Arbeit der Polizei zeigt jedoch oftmals ein anderes Bild. Erkenntnisse über potenzielle Gefährder oder Netzwerke entstehen nicht in einem Moment, sondern fragmentarisch und im Zeitverlauf. Sie können sich über Monate oder Jahre hinweg erstrecken. Typische Beispiele:

- Meldungen der Bundespolizei: Verdächtige Reisebewegungen einer Person an Grenzkontrollstellen
- Feststellungen an sensiblen Orten: Beobachtung einer Person an gefährdeten Objekten (kritische Infrastruktur, Regierungsgebäude)
- Ermittlungsergebnisse: Personen- und Fahrzeugkontrollen in verschiedenen Landesteilen
- Informationen von Dritten: Erkenntnismitteilungen von Nachbarn, Arbeitgebern oder Beratungsstellen
- Technische Auffälligkeiten: Kommunikationsmuster oder Internetchecks, die schrittweise zusammenfließen
- mehrfache polizeilich relevante Verhaltensauffälligkeiten

Jede dieser Informationen ist isoliert betrachtet in der Regel nicht aussagekräftig genug, um die hohe Schwelle einer „Negativprognose für künftige Straftaten von erheblicher Bedeutung“ zu erfüllen. Erst die kumulative Betrachtung im Zeitverlauf kann bedeutsam werden und eine rechtfertigende Prognose ermöglichen. Hierfür ist der Polizei ein angemessener Zeitrahmen für die Sammlungen, Zusammenfassung und Bewertung der Erkenntnisse und Informationen einzuräumen. Die Vergangenheit hat leidvoll gezeigt, wie notwendig das systematische Sammeln, Speichern und kumulative Analysieren fragmentarischer Erkenntnisse ist: Bei den Anschlägen am Breitscheidplatz (2016), in Hanau (2020) und in Halle (Saale) (2019) und insbesondere des Anschlages in Magdeburg (2024) verfügten die Behörden im Vorfeld über verstreute, teils niederschwellige Hinweise – Observationen, verdächtige Aktivitäten, auffälliges Verhalten, öffentliche Ankündigungen (Postings), Warnungen aus dem Ausland, Informationen aus dem Umfeld, Ansprachen –, die bei Zusammenführung und zeitlicher Verdichtung ein klares Gefährdungsbild ergeben hätten, aber nicht zu einer Gesamtschau verdichtet wurden. Dies gilt es zu verhindern und den rechtlichen Rahmen im Spannungsfeld der verfassungsrechtlichen Grenzen anzupassen, sonst droht die Gefahr des Verlustes der polizeilichen Gefahrenfrüherkennung. Im Zeitalter mehrdimensionaler, geopolitisch verursachter hybrider Bedrohungen, denen sich Sachsen stellen muss, gilt dies umso mehr. Ein auf diese Lage angepasstes Sächsisches Polizeivollzugsdienstgesetz stellt hierbei ein essentielles Element zur Lagebewältigung dar.

Neben den bereits skizzierten Bereichen: hybride Bedrohungen, Extremismusprävention und Terrorbekämpfung – wo fragmentarische Erkenntnisse oft das Primärsignal sind – werden polizeiliche Möglichkeiten mit der aktuellen Regelung auch in anderen Feldern unverhältnismäßig begrenzt. So gilt beispielsweise auch für den Bereich der häuslichen Gewaltprävention, dass eine Gefahrenprognose erst in der Summe der einzelnen Situationen, in den die Polizei gerufen wird, tragfähig wird. Mit der jetzigen Regelung kann die Polizei erst speichern, wenn eine Person bereits manifest strafrechtlich oder gefahrenabwehrrechtlich auffällig wurde – in vielen Situationen voraussichtlich ein klassisches Versagen bei der Gefahrenprävention und Gefahrenabwehr.

Darüber hinaus entstünden aus unserer Sicht potentiell auch tiefgreifende Probleme im Informationsverbund mit anderen Behörden. Es besteht die Gefahr, dass die sächsische Polizei vom Erkenntnisprozess, der in anderen Behörden stattfindet, abgekoppelt ist. Wechselseitige Fehleinschätzungen sind dann einzukalkulieren. Abschließend ist das Thema auch unter dem Blickwinkel effizienter Ressourcen sowie datenschutzrechtlicher Belange relevant. Bei neuen bzw. aufgrund mangelnder Speicherung als neu interpretierten Informationen besteht die Gefahr, dass Datenerhebungen, Analysen und Untersuchungen faktisch jeweils „von vorne“ beginnen, da die frühen Kontextdaten gelöscht sind. Dies führt oftmals zu mehrfachen Ermittlungen zu denselben Personen. Ob und inwieweit dies datenschutzrechtlich jeweils zu einer geringeren Eingriffsintensität und -tiefe im Vergleich zu einer eher kurzfristigen Speicherung führt, kann in Frage gestellt werden, denn eine begrenzte Speicherung mit klaren Regeln für eine Löschung ist datenschutzfreundlicher als das ständige Neusammeln von Informationen."

Mithin besteht aus Sicht des Bundes Deutscher Kriminalbeamter Änderungsbedarf. In diesem Kontext ist zu berücksichtigen, dass sich das Bundesverfassungsgericht in seinem Urteil vom 1. Oktober 2024 (1 BvR 1160/19) dieser Komplexität bewusst war.

Es hat im Zusammenhang zu der im Bundeskriminalamtsgesetz (BKAG) verankerten Prüfspeicherfrist Folgendes ausgeführt:

- Eine Prüfspeicherfrist ist verfassungsrechtlich zulässig und geboten
- Daten dürfen zunächst gespeichert werden, um dann – während dieser befristeten Frist – zu prüfen, ob die Speichervoraussetzungen (Negativprognose) vorliegen
- Dies ist ein angemessener Ausgleich zwischen Datenschutz und Sicherheit
- Die Prüfung muss dokumentiert werden, und nicht relevante Daten sind nach Ablauf der Frist zu löschen

Das seit 24. Juli 2025 in Kraft getretene BKAG hat die BVerfG-Vorgaben bereits umgesetzt. § 18 Abs. 3 BKAG regelt die explizite Prüfspeicherfrist (bis zu 12 Monate), um festzustellen, ob die Voraussetzungen der vorsorgenden Speicherung erfüllt sind. § 77 BKAG schafft darüber hinaus differenzierte Aussonderungsprüffristen (zwei Jahre für Erwachsene, ein Jahr für Jugendliche), die bei hinzutretenden Erkenntnissen verlängerbar sind. Dieses Modell ermöglicht es dem BKA, fragmentarische Informationen befristet zu sammeln und kumulativ zu analysieren, bevor entschieden wird, ob die Negativprognose vorliegt und eine dauerhafte Speicherung erforderlich ist.

Der Referentenentwurf des SächsPVDG schöpft diese verfassungsrechtliche Möglichkeit nicht aus, obwohl das BVerfG diese Regelungsweise ausdrücklich akzeptiert und auch der SächsVerfGH nicht verlangt, dass die Negativprognose bereits bei Speicherung vollständig vorliegen muss – nur dass sie tatsachenbefestigt sein muss, was auch durch eine Prüfung während einer befristeten Speicherphase erfolgen kann. Dies verschafft Sachsen im Bundesvergleich aus unserer Perspektive eines der aktuell restriktivsten Modelle: Der Entwurf kombiniert relativ kurze Speicherfristen mit der Anforderung einer sofortigen, vollständigen Negativprognose bereits bei Datenerfassung und restriktiver Zweckbindung. Sachsen bleibt damit erheblich hinter den von Bund und Ländern beschrittenen Wegen zurück.

Aus diesem Grund empfehlen wir die Einführung einer Prüfspeicherfrist nach dem Vorbild des Bundeskriminalamtsgesetzes:

„Die Polizei kann personenbezogene Daten, die im Rahmen ihrer Aufgabenerfüllung erhoben wurden, zunächst für eine Prüffrist von bis zu zwölf Monaten speichern, um zu prüfen, ob die Voraussetzungen des Absatz 1 Satz 2 erfüllt sind. Die durchgeführte Prüfung ist zu dokumentieren. Liegen die Voraussetzungen nach Ablauf der Prüffrist nicht vor, sind die Daten unverzüglich zu löschen. Die Prüffrist kann zweimal um bis zu weitere 6 Monate verlängert werden, wenn hinzutretende Erkenntnisse dies erforderlich machen oder der Grundsachverhalt erheblich erscheint.“

Die nähere Ausgestaltung könnte in einer ergänzenden Richtlinie geregelt werden.

Als alternative Option zur Einführung einer expliziten Prüfspeicherfrist wäre entsprechend zu erwägen, die Zweckbindungsregelungen oder die Verarbeitungsklausel so auszugestalten, dass die Daten in dem oben genannten Zeitraum für eine kumulative Analyse zur Gefahrenabwehr bzw. präventive Bewertung genutzt werden können.

Falls keine Änderungen an den Speicherregelungen des Referentenentwurfs vorgenommen werden, bleibt die Polizei in Sachsen dauerhaft darauf beschränkt, Informationen oftmals nur punktuell und isoliert zu dokumentieren, sodass regionale und überregionale Gefährdungslagen, Vernetzungen und frühzeitige Radikalisierungsprozesse regelmäßig unentdeckt bleiben – die sächsischen Sicherheitsbehörden wären damit in ihrer präventiven Handlungsfähigkeit eingeschränkt und stünden im Ernstfall vor dem Risiko, entscheidende Warnsignale zu übersehen.

2. Speicherfristen im Extremismus- und Terrorismusbereich

Der Bund Deutscher Kriminalbeamter erkennt an, dass § 80d Absatz 3 Nummer 3 SächsPVDG-E – mit einer Aussonderungsprüffrist von zwei Jahren bei Erwachsenen und ein Jahr bei Jugendlichen – dem BKAG-Standard und den Vorgaben des Bundesverfassungsgerichts (1 BvR 1160/19) entspricht. Dieses Modell stellt einen verfassungsgerechten Ausgleich dar. Allerdings weisen Radikalisierungsprozesse und Extremismus-Netzwerke andere Zeitdynamiken auf als klassische Strafermittlungsfälle: Inaktivitätsphasen sind kein Abkehrsignal, sondern Teil bewusster Tarnungsstrategien.

Das BVerfG-Urteil erlaubt eine Differenzierung „im Einzelfall und unter Berücksichtigung der spezifischen Gefahr.“ Dies zeigt sich im BKAG selbst: § 77 Absatz 8 Satz 6 BKAG gestattet bei schweren Straftaten nach § 100a Absatz 2 StPO eine unbegrenzte Verlängerung (mehr als zweimal). Diese Differenzierung wird begründet durch das Schutzzut – Leben, Freiheit und Staatssicherheit.

Empfehlung:

§ 80d Absatz 4 sollte daher ergänzt werden: „Bei Straftaten nach § 100a Absatz 2 Strafprozessordnung kann eine erneute Aussonderungsprüffrist unbegrenzt verlängert werden, wenn im Einzelfall fortbestehend tatsächliche Anhaltspunkte für die Prognose einer solchen Straftat vorliegen.“

3. Logik der Einwilligungregelung (§ 80a SächsPVDG-E)

Die im Entwurf vorgesehene Ausnahmeregelung des § 80a Abs. 1 Satz 2 SächsPVDG-E kann missverstanden werden, sie vermischt zwei rechtlich unterschiedliche Gefährdungsszenarios.

Zum einen besteht das Risiko, dass eine Person nicht zustimmen würde, obwohl die Polizei die Daten benötigt – etwa weil ein Zeuge aus Angst vor Vergeltung nicht einwilligen möchte oder ein Informant aus Sicherheitsgründen anonym bleiben will, oder weil die Person grundsätzlich gegenüber der Polizei datenschutzrechtliche oder sonstige Bedenken hat. Zum anderen kann das Bekanntwerden der Speicherung selbst den Speicherzweck gefährden, wenn etwa die Sicherheit der Person durch die Offenlegung gegenüber Dritten unmittelbar bedroht wäre.

Die Norm funktioniert nicht als Reaktionsregel, bei der erst gefragt und dann bei Ablehnung gespeichert wird. Sie ist vielmehr eine antizipative Befugnisregel – die Polizei muss bereits im Vorfeld prognostizieren, ob und aus welchem Grund eine Speicherung ohne Einwilligung erforderlich ist. Die geltende Formulierung führt jedoch zu Rechtsunsicherheit, da unklar bleibt, ob sie sich auf

die Offenbarung durch eine Nachfrage oder auf das bloße Bekanntwerden der Speicherung bezieht. Dies ermöglicht Missverständnisse und könnte zugleich bei zu breiter Auslegung zu willkürlichen Speicherungen führen.

Der BDK empfiehlt folgende Reformulierung:

§ 80a Abs. 1 Satz 2 SächsPVDG-E (empfohlene Neufassung):

Die vorsorgende Speicherung zu Personen nach Satz 1 Nummer 1 bis 3 darf ohne Einwilligung der Person erfolgen, wenn Anhaltspunkte dafür vorliegen, dass

- 1. die Person der Speicherung nicht zustimmen würde, die Polizei diese Daten aber zur Erfüllung ihrer Aufgaben benötigt, oder*
- 2. das Bekanntwerden der Speicherung den mit der Speicherung verfolgten Zweck gefährden würde.*

Die Gefährungsprognose und die Erforderlichkeit der Speicherung sind zu dokumentieren.

Diese Klarstellung schafft rechtliche Sicherheit für die Polizei und verhindert zugleich Missbrauch durch die Dokumentationspflichten. Die Reformulierung schafft Kohärenz mit Bundesrecht (§ 19 Abs. 1 BKAG) sowie mit Art. 6 der Richtlinie 2016/680/EU, wäre jedoch deutlich klarer formuliert.

4. Technische Befugnisse und Videotechnik (§§ 15, 57, 57a, 61 SächsPVDG-E)

Die Modernisierung technischer Befugnisse ist grundsätzlich zu begrüßen, bedarf jedoch präziserer und konsistenter Ausgestaltung:

§ 57 SächsPVDG-E (Bodycam): Klärung der Abgrenzung zu repressiven Maßnahmen (§ 163 StPO) sowie Vereinheitlichung der Gefahrenschwellen in Abs. 4 und 5.

§ 57 Abs. 9 SächsPVDG-E (Verkehrsaufnahmen): Präzisierung unbestimmter Begriffe wie „in regelmäßiger Weise“ oder „besondere Unfallträchtigkeit“.

§ 57a SächsPVDG-E (Mustererkennung / biometrische Fernidentifizierung): Die Norm ist sprachlich überfrachtet. Es braucht klare, handlungsleitende Begriffe und technische Mindeststandards (Bias-Tests, Fehlerraten-Grenzen, regelmäßige Audits).

§ 61 SächsPVDG-E (Elektronische Aufenthaltsüberwachung): Vereinheitlichung der Formulierungen („absehbarer Zeitraum“, „überschaubare Zukunft“) mit verbindlichen zeitlichen Orientierungswerten in der Verwaltungsvorschrift.

Ziel: Rechtsklarheit, Nachvollziehbarkeit und praktische Anwendbarkeit im polizeilichen Alltag.

5. Automatisierte Datenanalyse und KI-Systeme (§§ 62a SächsPVDG-E)

Die Schaffung einer eigenständigen Rechtsgrundlage für den Einsatz automatisierter Datenanalyseverfahren zur Gewinnung neuer Erkenntnisse wird seitens des Bundes Deutscher Kriminalbeamter ausdrücklich befürwortet. Sie entspricht den Vorgaben des Bundesverfassungsgerichts (Urteil vom 16. Februar 2023, Az. 1 BvR 1547/19 u. a.) und adressiert korrekt die eingriffsintensiven Verfahren des systematischen Zusammenführens und Verknüpfens bislang unverbundener Datenbestände zur Generierung neuer Verdachtsmomente. Die Vorschrift bildet somit einerseits die Grundlage für den Einsatz moderner Analyseverfahren, schränkt diese andererseits faktisch stark ein.

Denn der Entwurf trägt zunächst die Gefahr erheblicher praktischer Rechtsunsicherheit für die erforderliche Modernisierung polizeilicher Arbeit. Der fehlende explizite Unterschied zwischen eingriffsintensivem Verfahren einerseits und technischen Unterstützungssystemen andererseits schafft Auslegungsspielräume, die zu Blockierungen notwendiger digitaler Entwicklungen führen können. Hier besteht das Erfordernis einer klaren Abgrenzung.

In der Praxis werden derzeit computergestützte Assistenzsysteme entwickelt und erprobt – beispielsweise für das polizeiliche Gefahrenmanagement –, die Sachbearbeiter durch Aufbereitung, Strukturierung und Zusammenfassung unstrukturierter Textdokumente unterstützen oder ähnlich einer Suchfunktion auf vordefinierte Risikofaktoren hinweisen. Diese Systeme zeichnen sich dadurch aus, dass sie

- keine eigenständige Risikobewertung, Prognose oder Scoring-Entscheidung treffen,
- ausschließlich die Verarbeitung bereits rechtmäßig erhobener Daten im Rahmen des ursprünglichen Erhebungszwecks unterstützen, und
- alle Bewertung und Entscheidung vollständig beim menschlichen Sachbearbeiter belassen.

Solche Systeme sind in ihrer Eingriffstiefe und ihrem Gefahrenpotenzial fundamental von den Maßnahmen des § 62a SächsPVDG-E verschieden, die gerade auf die automatisierte Generierung neuer Erkenntnisse aus der Zusammenführung unverbundener Datenbestände abzielen. Der Umstand, dass der Gesetzgeber durch § 62a SächsPVDG-E eine hohe Eingriffsrechtfertigung für die systematische maschinelle Datenanalyse zur Gewinnung neuer Verdachtsmomente schafft, impliziert im Umkehrschluss, dass niedrighschwellige Assistenzsysteme als „Minusmaßnahmen“ nicht unter diese Spezialregelung fallen. Um Rechtssicherheit für die polizeiliche Modernisierung zu schaffen, wird die Aufnahme einer expliziten Klarstellung empfohlen. Ohne eine ausdrückliche Klarstellung besteht das Risiko, dass eine zu weite Auslegung des § 62a SächsPVDG-E erforderliche digitale Entwicklungen faktisch blockiert.

Die Verwaltungsvorschrift nach § 62a Abs. 4 SächsPVDG-E ist hierfür nicht ausreichend. Die Klarstellung sollte entweder direkt im Gesetzestext (als Absatz 7 in § 62a) oder in der amtlichen Gesetzesbegründung erfolgen:

„Der Anwendungsbereich des § 62a SächsPVDG-E erfasst nicht technische Unterstützungssysteme und Assistenzsoftware, die lediglich der Aufbereitung, Strukturierung, Filterung oder Visualisierung

von Daten dienen, welche die Polizei bereits rechtmäßig erhoben hat und die im Rahmen ihres ursprünglichen Erhebungszwecks verarbeitet werden. Dies betrifft insbesondere Systeme, die

- *keine eigenständige Risikobewertung, Gefährlichkeitsprognose oder automatisierte Scoringentscheidung durchführen,*
- *ausschließlich der Unterstützung der menschlichen Bearbeitung dienen (z. B. Textzusammenfassung, kontextsensitive Recherche, Datenaufbereitung),*
- *nach dem Prinzip der menschlichen Kontrolle und Entscheidungskompetenz ausgestaltet sind, und*
- *nicht zu neuen Erkenntnissen durch Verknüpfung bislang unverbundener Datenbestände führen.*

Für solche Systeme bleibt der rechtliche Ordnungsrahmen durch die allgemeinen datenschutzrechtlichen Bestimmungen – insbesondere die Anforderungen an Errichtungsanordnungen nach § 93 SächsPVDG und Datenschutz-Folgenabschätzungen – sowie durch die Künstliche-Intelligenz-Verordnung der Europäischen Union unberührt. Eine Inanspruchnahme von § 62a SächsPVDG-E ist für diese Systeme nicht erforderlich.“

Weitere Problemfelder im Zusammenhang mit der Anwendung des § 62a SächsPVDG-E stellen aus unserer Perspektive die „Identifizierung unbekannter Täter im Anlassfall (§ 62a Abs. 1 Nr. 2)“, die „Verwendung von Verkehrsdaten im Bereich Terrorismus-Vorfeld (§ 62a Abs. 3 Satz 5)“, die „Automatisierte Auswertung öffentlich zugänglicher Internetquellen (§ 62a Abs. 3 Satz 4)“, die „Definition verbindlicher technischer Standards (§ 62a Abs. 4)“ und der „Regelungsinhalt bezüglich des Personal- und Schulungsbedarfs für lernende Systeme (§ 62a Abs. 4 Satz 2)“ dar.

Verwendung von Verkehrsdaten im Bereich Terrorismus-Vorfeld (§ 62a Abs. 3 Satz 5 SächsPVDG-E)

Das absolute Verbot von Verkehrsdaten bei präventiven Maßnahmen zur Terrorismusbekämpfung steht in analytischer Widersprüchlichkeit zur praktischen Notwendigkeit dieser Daten gerade in der höchsten Sicherheitslage. Nach geltender Regelung darf die Polizei bei terroristischen Vorfeldstraftaten nach § 89a StGB keine Verkehrsdaten – weder Funkzellendaten noch Bewegungsprofile – in die Datenanalyse einbeziehen. Dies stellt sich als besonders problematisch dar, weil solche Daten gerade in diesem Bereich analytisch von höchster Relevanz sind. Verkehrsdaten zeigen zuverlässig: Wo halten sich verdächtige Personen auf? Treffen sie sich wiederholt an denselben Orten? Wer kommt hinzu? Diese Informationen stellen für die Terrorbekämpfung etablierte und bewährte Erkenntnisquellen dar.

Die formale Begründung für diese restriktive Regelung lautet, dass die Eingriffsschwelle beim Terrorismus-Vorfeld („konkretisierte Gefahr“) niedriger liegt als bei konkreten Straftaten, mithin der zulässige Umfang der Eingriffe geringer sein müsse. Diese Logik ist verfassungsrechtlich nachvollziehbar. Sie vernachlässigt jedoch die sicherheitspolitische Realität: Terrorismus stellt die höchste nationale Sicherheitslage dar. Gerade in dieser Situation darf die Polizei nicht faktisch handlungsunfähig gemacht werden. Unter verstärkter Dokumentation und richterlicher Kontrolle sollten Verkehrsdaten auch bei Vorfeldmaßnahmen nutzbar sein. Dies würde einen angemessenen Ausgleich zwischen Sicherheitsinteressen und Grundrechtsschutz gewährleisten.



Empfehlung:

§ 62a Absatz 3 Satz 5 SächsPVDG-E sollte wie folgt ergänzt werden: „Verkehrsdaten dürfen bei Maßnahmen nach Absatz 1 Nummer 3 ausnahmsweise einbezogen werden, sofern im Einzelfall richterlich angeordnet und dokumentiert ist, dass sie für die begründete Prognose einer terroristischen Straftat unerlässlich sind.“

Automatisierte Auswertung öffentlich zugänglicher Internetquellen (§ 62a Abs. 3 Satz 4 SächsPVDG-E)

Die Regelung untersagt eine direkte maschinelle Anbindung an Internetquellen und macht damit die systematische Erfassung von Rekrutierungs- und Organisationsprozessen in sozialen Medien praktisch unmöglich. Die derzeitige Regelung verbietet praktisch eine direkte Anbindung automatisierter Analysesysteme an Internetquellen. Dies bedeutet operativ: Die Polizei kann nicht automatisiert in sozialen Medien oder Messenger-Diensten recherchieren. Stattdessen muss sie relevante Daten einzeln extrahieren, gesondert speichern und manuell eingeben. Diese Vorgehensweise stellt bei der Bekämpfung von Extremismus eine erhebliche operative Beschränkung dar. Radikale und terroristische Gruppen rekrutieren und organisieren sich nachweislich über Plattformen wie Telegram, TikTok und Discord – diese Daten sind öffentlich verfügbar. Sie sollten methodisch durchsuchbar sein. Die gegenwärtige Regelung erzwingt stattdessen die manuelle Extraktion einzelner Posts – bei hunderten oder tausenden potenzieller Treffer pro Jahr faktisch nicht realisierbar.

Das Bundesverfassungsgericht hat in seinem Urteil zur automatisierten Datenanalyse vom 16. Februar 2023 (Az. 1 BvR 1547/19, 1 BvR 2634/20) klargestellt, dass daten- und methodenoffen formulierte Befugnisse, die eine unkontrollierte Verarbeitung unbegrenzter Datenbestände ermöglichen, gegen das Grundrecht auf informationelle Selbstbestimmung verstoßen. Es existiert jedoch gegebenenfalls ein verfassungskonformer Mittelweg: automatisierte Auswertung mit normklaren, eng begrenzten Suchparametern, vollständiger Protokollierung und Mengenbegrenzung

Empfehlung:

Eine präzisierende Klarstellung sollte festlegen, dass automatisierte Auswertung öffentlich zugänglicher Internetquellen zulässig ist, wenn die Daten tatsächlich öffentlich einsehbar, einzel-fallbezogen ausgewählt und vollständig protokolliert sind. Diese Klarstellung sollte in der Gesetzesbegründung zu § 62a Absatz 3 Satz 4 SächsPVDG-E oder durch ergänzende Regelung erfolgen.

Definition verbindlicher technischer Standards (§ 62a Abs. 4 SächsPVDG-E)

Die Delegation technischer Qualitätsstandards an Verwaltungsvorschriften erzeugt Rechtsunsicherheit bei Systemanbietern und lässt das strukturelle Black-Box-Problem bei selbstlernenden Systemen ungelöst. § 62a Absatz 4 SächsPVDG-E delegiert die Festlegung technischer Standards an nachgeordnete Verwaltungsvorschriften. Während Technologieoffenheit ein berechtigtes Regulierungsprinzip ist, entsteht dadurch erhebliche Rechtsunsicherheit für Softwarehersteller und externe Systementwickler.

Ein fundamentales Problem besteht bei selbstlernenden KI-Systemen: Bei neuronalen Netzen ist häufig unklar, durch welche Mechanismen der Algorithmus zu seinen Ergebnissen gelangt (das sogenannte Black-Box-Problem). Viele KI-Systeme reproduzieren unbewusst und systematisch Verzerrungen aus ihren Trainingsdaten. Wenn historische Polizeidaten bestimmte Bevölkerungsgruppen überrepräsentativ erfassten, lernt das Modell diese Muster und wird damit strukturell diskriminierend – ohne dass dies bewusst programmiert wurde. Die Verwaltungsvorschrift verlangt zwar formal ein Diskriminierungsverbot, präzisiert dies aber nicht technisch und operational. Sie müsste konkrete Testverfahren, regelmäßige Audits und objektive Schwellenwerte für zulässige Fehlermargen vorgeben.

Empfehlung:

Die Gesetzesbegründung zu § 62a Absatz 4 SächsPVDG-E sollte verbindliche technische Mindeststandards explizit festlegen: lückenlose Protokollierung jeder Datenabfrage mit Zeitstempel, Nutzer-Identifikation, Suchmuster, Ergebnis und Datenempfänger; automatisiertes Audit-Reporting mindestens monatlich mit systematischer Analyse auf Anomalien und Missbrauchsindikatoren; etabliertes Verfahren zur Identifikation und Korrektur fehlerhaft gelöschter oder unberechtigt gespeicherter Datensätze; operative Schnittstelle zur Datenschutzbehörde für zeitnahe Meldung von Systemfehlern und technischen Anomalien.

Regelungsinhalt bezüglich des Personal- und Schulungsbedarfs für lernende Systeme (§ 62a Abs. 4 Satz 2 SächsPVDG-E)

Der Entwurf verlangt spezialisierte Qualifikation für den Zugriff auf automatisierte Analysesysteme, trifft aber keine verbindlichen Aussagen darüber, wie diese Qualifikation erworben, dokumentiert und aufrechterhalten wird. Der operative Einsatz von KI-gestützter automatisierter Datenanalyse erfordert spezialisiertes und qualifiziertes Personal – sowohl für die sachgerechte Bedienung der Systeme als auch für die fachlich korrekte Interpretation und kritische Überprüfung von Analyseergebnissen. Der Referentenentwurf sieht vor, dass Zugriffsrechte eingeschränkt nach „Phänomenbereichen, Funktion und spezifischer Qualifikation“ vergeben werden (§ 62a Absatz 4 Satz 2 SächsPVDG-E). Die Regelung trifft jedoch keine verbindliche Aussage darüber, wie diese erforderliche Qualifikation konkret definiert, erworben und aufrechterhalten wird.

Dadurch entstehen erhebliche operative Risiken. Das Gesetz schafft eine Befugnis für hochkomplexe Analyseverfahren, ohne zu regeln, wie die Polizeibediensteten fachlich dafür ausgebildet werden. Dies führt unvermeidlich zu Bedienungsfehlern, Fehlinterpretationen von algorithmischen Ergebnissen und potenziellen Missbrauchsmöglichkeiten. Spezialisierte Schulung ist essential, um Funktionsweisen, technische Grenzen, algorithmische Fehlerquellen und latente Bias-Risiken zu verstehen.

Empfehlung:

Eine Verwaltungsvorschrift oder präzisierende Regelung in der Gesetzesbegründung sollte verbindliche Schulungs- und Qualifikationsstandards festlegen: Polizeibedienstete mit Zugriff auf

automatisierte Datenanalyseverfahren müssen eine dokumentierte Grundschulung zu Funktionsweisen, technischen Grenzen, algorithmischen Fehlerquellen und Bias-Risiken absolvieren; regelmäßige Auffrischungsschulungen sind mindestens alle zwei Jahre erforderlich; ein systematischer Qualitätssicherungsprozess muss etabliert werden, nach dem Analyseergebnisse stichprobenartig validiert und überprüft werden; die erforderlichen Schulungs- und Personalkosten sind in den Haushaltsmitteln der sächsischen Polizei angemessen zu veranschlagen.

Zusammenfassung unserer Empfehlungen:

Abgrenzung technischer Assistenzsysteme: Klarstellung, dass technische Unterstützungssysteme und Assistenzsoftware, die lediglich Aufbereitung, Strukturierung, Filterung oder Visualisierung bereits erhobener Daten dienen, nicht unter § 62a SächsPVDG-E fallen (als Absatz 7 in § 62a SächsPVDG-E oder in der Gesetzesbegründung)

Terrorismusprävention: Ausnahmeregelung für Verkehrsdaten unter richterlicher Anordnung, Kontrolle und dokumentierter Erforderlichkeitsprüfung (§ 62a Abs. 3 Satz 5 SächsPVDG-E)

Internetquellen: Zulassung automatisierter Auswertung öffentlich zugänglicher Quellen mit vordefinierten Suchparametern, mengenmäßiger Begrenzung und vollständiger Protokollierung (§ 62a Abs. 3 Satz 4 SächsPVDG-E)

Technische Standards: Festlegung verbindlicher Mindeststandards für Protokollierung, Audit-Frequenz, Diskriminierungsprüfung und Fehlerbehandlung in der Gesetzesbegründung (§ 62a Abs. 4 SächsPVDG-E)

Schulung und Qualifikation: Bindende Schulungsanforderungen mit definierten Auffrischungsintervallen, Qualitätskontrollprozessen und angemessener Haushaltsveranschlagung (§ 62a Abs. 4 Satz 2 SächsPVDG-E)

Mit den vorstehend dargestellten Klarstellungen würde § 62a SächsPVDG-E ein praxistaugliches und verfassungskonformes Regelwerk bilden. Der Referentenentwurf schafft grundsätzlich die konzeptionell richtige, wertvolle Grundlage – Gewährleistung von Rechtssicherheit für automatisierte Datenanalyse unter Beachtung des Grundrechtsschutzes. Dieser positive konzeptionelle Ansatz wird jedoch durch erhebliche praktische Unklarheiten und regulatorische Lücken beeinträchtigt. Die Regelung wird systemisch zu restriktiv und rechtlich zu unpräzise gerade dort, wo die sächsische Polizei die erforderlichen Befugnisse zur effektiven Aufgabenerfüllung am dringendsten benötigt: bei der Bekämpfung terroristischer Bedrohungen, bei der Prävention von Extremismus sowie bei der Aufklärung komplexer krimineller Netzwerkstrukturen.

Ohne die vorgeschlagenen Ergänzungen besteht das erhebliche Risiko eines regulatorischen Paradoxons: Die Vorschrift wird zwar formell verabschiedet, in der praktischen Anwendung aber faktisch wirkungslos. Dies würde den Freistaat Sachsen beim erforderlichen Modernisierungsprozess der polizeilichen Arbeit erheblich benachteiligen und die Schlagkraft der Sicherheitsbehörden einseitig schwächen. Eine zügige Nachbesserung durch Gesetzesbegründung oder ergänzende Regelungen ist daher dringend erforderlich.

6. Quellen-Telekommunikationsüberwachung (§ 66 SächsPVDG-E)

Die derzeit vorgesehene Schwelle der „gegenwärtigen Gefahr“ wird in der Praxis kaum erreicht werden und die Anwendung faktisch ausschließen. § 66 Absatz 2a Nummer 1 SächsPVDG-E verlangt für die Quellen-TK das Vorliegen einer „gegenwärtigen Gefahr“ für klar definierte Rechtsgüter (Bestand oder Sicherheit des Bundes oder eines Landes, Leib, Leben oder Freiheit einer Person, oder Sachwerte von erheblicher Bedeutung im öffentlichen Interesse). Dies stellt eine deutlich höhere Anforderung dar als bei der konventionellen Telekommunikationsüberwachung nach § 66 Absatz 1 SächsPVDG-E, die bereits bei der Annahme einer bloßen „konkretisierten Gefahr“ zulässig ist. Eine gegenwärtige Gefahr erfordert, dass die Bedrohung unmittelbar bevorzustehen scheint – ein Zustand, der gerade bei der Terrorismusprävention und bei der Bekämpfung organisierter Kriminalität selten eintritt, wenn es um die Aufdeckung von Organisationsstrukturen und Kommunikationsnetzen geht. Der Gesetzgeber hat damit zwar eine starke Schutzregelung geschaffen, aber gleichzeitig ein regulatorisches Hindernis etabliert, das die Praktikabilität der Quellen-TK als tatsächliches Ermittlungsinstrument erheblich gefährdet. Dies ist besonders problematisch, da gerade die Quellen-TK als technisches Verfahren zur Entschlüsselung verschlüsselter Kommunikation in modernen Ermittlungen essential ist – aber nur dann sinnvoll einsetzbar ist, wenn die Schwelle nicht prohibitiv hoch angesetzt ist.

Empfehlung:

Bereits in der Gesetzesbegründung sollte eine spätere Überprüfung der Eingriffsschwelle („konkretisierte Gefahr“) vorgesehen werden, falls sich die Maßnahme als nicht praktikabel erweist.

7. Datenübermittlung im innerstaatlichen Bereich (§ 84 SächsPVDG-E)

Die gegenwärtige Fassung von § 84 Absatz 3 SächsPVDG-E konzentriert sich ausschließlich auf einen reaktiven Opferschutzansatz und verwehrt der Polizei damit ein etabliertes Interventionsinstrument zur Reduzierung von Rückfallquoten bei Gewaltdelikten. Hier besteht offensichtlich eine Regelungslücke bei der Datenübermittlung.

Die Regelung nach § 84 Absatz 3 Satz 1 Nummer 4 und Satz 2 SächsPVDG-E schafft zwar eine Rechtsgrundlage für die Übermittlung von Personendaten an spezialisierte Beratungsstellen im Bereich häuslicher Gewalt, limitiert diese jedoch auf Situationen, in denen ein Schutzbedarf der angegriffenen oder gefährdeten Person nachgewiesen ist. Dies ist ein gerechtfertigter Opferschutzfokus. Die Regelung übersieht jedoch die präventiven Effekte einer frühzeitigen Täterintervention unmittelbar im Anschluss an eine Straftat oder einen Verdachtsfall.

Die kriminologische Forschung sowie die praktische Erfahrung von Gewaltpräventionsprogrammen zeigen, dass Täterberatung und spezialisierte Täterarbeit signifikant zur Prävention von Rückfalltaten beitragen. Ein Polizeieinsatz schafft dabei ein zeitliches und psychologisches Fenster der Zugänglichkeit: Der Beschuldigte/die Täterin ist konfrontiert mit den unmittelbaren Folgen seines/ihrer Handelns und kann in diesem Moment leichter für professionelle Unterstützungsangebote erreicht werden. Eine Situation, in der die Polizei bereits vor Ort ist und der Betroffene selbst einwilligen könnte, seine Daten an eine Fachberatungsstelle weitergeleitet zu erhalten,

würde einen niedrigschwelligen Zugang zu spezialisierter Beratung ermöglichen – ohne polizeilichen Zwang, aber mit hohem Präventionspotenzial für Wiederholungstaten.

Gerade angesichts der gestiegenen Inzidenzen im Bereich interpersonaler Gewaltdelikte und Belästigungsverstöße stellt dies eine regulatorische Lücke dar, die einer doppelten Prävention – zum Schutz von Opfern wie auch zur Unterstützung von Täterpersonen – entgegensteht.

Empfehlung:

§ 84 Absatz 3 SächsPVDG-E sollte um eine neue Nummer 5 ergänzt werden:

"5. zur Ermöglichung einer präventiven Kontaktaufnahme durch eine von dem Staatsministerium für Soziales, Gesundheit und Gesellschaftlichen Zusammenhalt bestimmte spezialisierte Beratungsstelle mit einer beschuldigten Person im Kontext von Gewalt- oder Belästigungsdelikten, wenn diese ausdrücklich und schriftlich in die Datenübermittlung eingewilligt hat und unter Berücksichtigung der Fallumstände Anlass besteht anzunehmen, dass eine professionelle Täterberatung zur Verhaltensänderung und zur Verhinderung zukünftiger Straftaten sinnvoll ist. Die empfangende Beratungsstelle darf die Daten ausschließlich dazu nutzen, die betreffende Person zu kontaktieren und ihr Beratungs- und Unterstützungsangebote zur Aufarbeitung des Verhaltens zu unterbreiten."

Eine solche Regelung würde der Polizei ein Präventionsinstrument an die Hand geben, das wissenschaftlich bewährt und praktisch bewährt ist, ohne dabei Grundrechte zu beeinträchtigen.

8. Zusammenfassende Bewertung

Der Gesetzentwurf ist juristisch ambitioniert und technologisch definitiv auf der Höhe der Zeit. Allerdings droht durch teilweise übermäßige Komplexität, zu enge Grenzen und unklare Formulierungen eine praktische Entwertung einzelner Befugnisse. In einigen Fällen (Speicherbefugnisse) besteht die Gefahr, dass die sächsische Polizei Teile ihrer Kernaufgaben nur noch unzureichend erfüllen kann und im Hinblick auf technologische Entwicklungen trotz ambitionierter Ansätze nicht schritthalten kann.

Der BDK Sachsen empfiehlt daher insbesondere:

1. Einführung einer Prüfspeicherfrist (12 + 6 Monate) nach BKAG-Vorbild oder analoge Regelung,
2. Verlängerung der Speicherfristen bei Extremismus- und Terrorismusbezug,
3. Klarstellung der Einwilligungsregelung in § 80a SächsPVDG-E,
4. Konsistenz und Präzisierung bei technischen Befugnissen (§§ 57, 57a, 61 SächsPVDG-E),
5. Praxistaugliche Ausgestaltung der automatisierten Datenanalyse (§§ 62a SächsPVDG-E),
6. Herabstufung der Gefahrenstufe bei der Quellen-Telekommunikationsüberwachung (§ 66 SächsPVDG-E)
7. Verbesserung der Regelungen zur Datenübermittlung im innerstaatlichen Bereich
8. Verbindliche Ressourcen- und Evaluierungsplanung für neue Technologien.



Diese Anpassungen schaffen Rechtsklarheit und Handlungssicherheit, ohne den rechtsstaatlichen Rahmen zu überschreiten. Das novellierte SächsPVDG kann ein modernes, verfassungstreues und zugleich praktikables Polizeigesetz werden, wenn auch die vorgenannten Punkte berücksichtigt werden.

Der BDK Sachsen appelliert an den Gesetzgeber, die Erfahrungen der polizeilichen Praxis ernst zu nehmen:

Rechtsstaatlichkeit ist die Grundlage – Handlungsfähigkeit ihr Garant!

Mit freundlichen Grüßen

Torsten Schmorte
Landesvorsitzender



Bundesanstalt Technisches Hilfswerk, Landesverband Sachsen, Thüringen,
Geschwister-Scholl-Straße 2, 04600 Altenburg

Sächsisches Staatsministerium des Innern
01095 Dresden

Janine Stock
Landesbeauftragte
Geschwister-Scholl-Straße 2
04600 Altenburg
Tel. +49 228-994581-100
Fax +49 3447-5684-180
Poststelle.LVSNTH@thw.de
<https://www.lv-snth.thw.de>

Betreff: Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG);

Anhörung des Referentenentwurfes

Bezug: Stellungnahme, E-Mail

Geschäftszeichen: SN, TH - 36-2002/25/14

Datum: Altenburg, 14.11.2025

Sehr geehrte Damen und Herren,

hiermit nehmen wir Stellung zur Novellierung des Sächsischen Polizeivollzugsdienstgesetzes. Der THW Landesverband Sachsen, Thüringen begrüßt die Novellierung und die damit verbundene Stärkung und Sicherung des Polizeivollzugsdienstes.

Insbesondere unterstützen wir die Paragraphen § 3 Tätigwerden für andere Stellen, § 12a Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme, § 71 Einsatz von unbemannten Luftfahrtsystemen (Unterstützung von Drohnen Überblickaufnahmen des Einsatzgeschehen und Übermittlung der Bildaufnahmen (an das THW ggf. i.V.m.), § 57 I II), § 79 Befugnis zur Datenverarbeitung, § 84 Datenübermittlung im innerstaatlichen Bereich (Absatz 2 Datenaustausch zwischen THW und Polizei) mit THW-Bezug.

Die Bundesanstalt THW ist eine Bundesbehörde, die sich auf technisch-humanitäre Hilfeleistungen spezialisiert hat. Die rund 3.000 ehrenamtlichen Helferinnen und Helfer des Landesverbandes Sachsen, Thüringen engagieren sich unter anderem bei Naturkatastrophen und Unfällen sowie Notlagen im In- und Ausland. Die Zusammenarbeit mit der sächsischen Polizei spielt dabei eine große Rolle und im Jahr 2025 konnten wieder zahlreiche Einsatzstunden bei der Abwehr von Gefahren geleistet werden.

Mit freundlichen Grüßen

Bitte wählen Sie aus.

gez.

Janine Stock

Verband sächsischer Verwaltungsrichterinnen und Verwaltungsrichter

Verband sächsischer Verwaltungsrichterinnen
und Verwaltungsrichter, Ortenburg 9, 02625 Bautzen

Sächsisches Staatsministerium
des Innern
Referat 36
Anhoerung.SaechsPVDG@smi.sachsen

Vorsitzender:
Dr. Matthias Mittag
Sächsisches Obergerverwaltungsgericht
Ortenburg 9
02625 Bautzen

Telefon: (03591) 2175 321
Telefax: (03591) 2175 500

Bautzen, den 20. November 2025

Novellierung des Sächsischen Polizeivollzugsdienstgesetzes hier: Verbandsstellungnahme

Ihr Az.: 36-2002/25/14

Sehr geehrte Damen und Herren,

für die Gelegenheit zur Stellungnahme zu der beabsichtigten Änderung des Sächsischen Polizeivollzugsdienstgesetzes danken wir. Wir nehmen diese Gelegenheit gerne wahr, weisen aber darauf hin, dass wir den Entwurf nicht in allen Einzelheiten einer Prüfung unterziehen konnten. Wir enthalten uns auch einer rechtspolitischen Diskussion über die Verfassungsmäßigkeit etwa der Quellen-TKÜ und beschränken uns auf folgende Punkte:

1. Die im Anschreiben angesprochene Möglichkeit, das Schutzgut der öffentlichen Ordnung wieder in den Tatbestand des § 18 SächsPVDG (Platzverweisung) aufzunehmen, sehen wir - wie den Rückgriff auf die öffentliche Ordnung im Gefahrenabwehrrecht insgesamt - kritisch. Das Schutzgut der öffentlichen Sicherheit hat nach § 4 Nummer 1 SächsPVDG einen bereits denkbar weiten Anwendungsbereich und dürfte in jeder Gefahrensituation ein angemessenes Einschreiten des Polizeivollzugsdienstes ermöglichen. Das Schutzgut der öffentlichen Ordnung erfasst nach der Legaldefinition des § 4 Nummer 2 SächsPVDG die „Gesamtheit der ... ungeschriebenen Regeln für das Verhalten von Personen in der Öffentlichkeit, deren Beachtung nach den jeweils herrschenden Anschauungen als unerlässliche Voraussetzung eines geordneten Zusammenlebens betrachtet wird“. Es müsste u. E. plausibel dargelegt werden, in welchen Fällen, die nicht bereits jetzt vom Tatbestand von § 18 SächsPVDG erfasst sind, ein Rückgriff auf dieses weite und nur wenig eingegrenzte Schutzgut erforderlich sein soll.

2. Die meisten Änderungen gehen auf Entscheidungen des Sächsischen Verfassungsgerichtshofs (Urt. v. 25. Januar 2024 - Vf. 91-II-19 -) sowie des Bundesverfassungsgerichts (u. a. Urt. v. 1. Oktober 2024 - 1 BvR 1160/19 - BKAG II; Urt. v. 27. Mai 2020 - 1 BvR 1873/13 u. a. -) zurück und dienen insbesondere der Umsetzung der im Urteil des Verfassungsgerichtshofs angemahnten Änderungen innerhalb der in Ziffer 12 des Tenors genannten Frist (30. Juni 2026). Die beabsichtigten Änderungen sind in großen Teilen durch eine zum Teil erhebliche Komplexität gekennzeichnet. Uns ist bewusst, dass diese Komplexität weitgehend auf verfassungsrechtlichen Anforderungen und auf den o. g. Entscheidungen des Sächsischen Verfassungsgerichtshofs sowie des Bundesverfassungsgerichts beruht. Trotzdem bleiben gewisse Zweifel, ob die Vorschriften praxistauglich und umsetzbar sind.

3. Durch Artikel 1 Nummer 3 soll in § 4 Nummer 5 SächsPVDG die Definition des Begriffs der terroristischen Straftat im Hinblick auf die Entscheidung des Verfassungsgerichtshofs eingegrenzt werden. Damit wird zugleich der Anwendungsbereich der Anknüpfungstatbestände (z. B. § 21 Abs. 2 SächsPVDG) verengt. Dies entsprach einer Forderung des Verfassungsgerichtshofs, wonach diese Anknüpfungstatbestände nicht mit der Sächsischen Verfassung vereinbar sind, soweit die in ihnen in Bezug genommenen Straftatbestände - wie nach der derzeitigen Fassung - auch Vorbereitungshandlungen und bloße Rechtsgutsgefährdungen erfassen. Diese Einengung ist im Grundansatz zu begrüßen.

Erstmals im Wege einer Legaldefinition soll mit § 4 Nummer 6 SächsPVDG-E die Vorfeldstraftat bestimmt werden. Damit wird das Regelungskonzept geändert. Denn das Merkmal der Vorfeldstraftat soll nach der Neukonzeption wiederum Anknüpfungstatbestände, also Eingriffsermächtigungen für konkrete polizeiliche Maßnahmen, einschränken (z. B. § 21 Abs. 2 Satz 2 SächsPVDG-E: „Soweit es sich bei ... um eine Vorfeldstraftat handelt, ist eine Maßnahme nur zulässig, wenn im Einzelfall tatsächliche Anhaltspunkte für ... vorliegen“). Dieses Regelungsmodell erscheint uns nicht ungeeignet, die Anforderungen der verfassungsgerichtlichen Rechtsprechung zu erfüllen. Allerdings haben wir gewisse Zweifel, ob die derart gestalteten Eingriffsermächtigungen in der Praxis noch gut gehandhabt werden können (s.o. 2.).

4. In Artikel 1 Nummer 5 heißt es zu § 15 Abs. 1 Satz 1 Nr. 7 SächsPVDG-E auszugsweise:

„...oder nach § 31a des Sächsischen Polizeibehördengesetzes zu verhindern, da Tatsachen die Annahme rechtfertigen, dass dann dort Straftaten dieser Art bevorstehen; ...“.

Das auf einen Kausalzusammenhang hinweisende Wort „da“ sollte bei der Formulierung von Tatbestandsvoraussetzungen durch das Wort „wenn“ ersetzt werden. Das Wort „dann“ sollte gestrichen werden, es hat an dieser Stelle keine Funktion. Wir schlagen daher alternativ vor:

„...oder nach § 31a des Sächsischen Polizeibehördengesetzes zu verhindern, wenn Tatsachen die Annahme rechtfertigen, dass dort Straftaten dieser Art bevorstehen; ...“

5. Mit Artikel 1 Nummer 6 soll die Wohnungsverweisung in § 19 SächsPVDG geändert werden. Der Ansatz, weitere Standardbefugnisse zum Schutz vor häuslicher Gewalt einzuführen, wird mit Blick auf die Istanbul-Konvention begrüßt. Die Absenkung der Gefahrenschwelle von der gegenwärtigen auf eine „bloße“ konkrete Gefahr erscheint uns vor dem Hintergrund der Schwere des in Rede stehenden Eingriffs hingegen nicht ganz unbedenklich, dürfte aber im Hinblick auf die ohnehin geltenden Anforderungen des Verhältnismäßigkeitsgrundsatzes verfassungsrechtlich zulässig sein. Uneingeschränkt begrüßt wird, dass die Anknüpfung „aus ihrer Wohnung“ (§ 19 Abs. 1 SächsPVDG in der geltenden Fassung) durch die Formulierung „gemeinsam mit der gefährdeten Person genutzten Wohnung“ ersetzt wird. Dies ermöglicht es, den Tatbestand auf Sachverhalte anzuwenden, in denen dies bislang nicht möglich war (vgl. Urt. des VG Leipzig v. 25.03.2025 - 3 K 403/24 -, juris).

6. Artikel 1 Nummer 13 hat u. a. den offenen Einsatz technischer Mittel zur Bild- und Tonaufnahme und -aufzeichnung zum Gegenstand (§ 57 SächsPVDG-E). § 57 Abs. 4 SächsPVDG-E soll den Einsatz von Bodycams mittels sog. Pre-Recordings regeln. Satz 1 entspricht im Wesentlichen der bisherigen Regelung. Satz 2 enthält Sondervorschriften für Wohnungen, während Satz 3 hiervon wiederum Ausnahmen für öffentlich zugängliche Betriebs- und Geschäftsräume während der Öffnungszeiten vorsieht. Insofern jedenfalls in der Begründung (S. 67), klargestellt werden, dass für diese Räume wiederum Satz 1 gelten soll. Im Übrigen ist eine solche Vorschrift nicht (nur) wegen der Weite des Wohnungsbegriffs des § 29 Abs. 5 SächsPVDG erforderlich (so die Begründung S. 67), vielmehr umfasst der Wohnungsbegriff des Grundgesetzes seinerseits die öffentlich zugänglichen Betriebs- und Geschäftsräume.

7. In Artikel 1 Nummer 19 (§ 66 Abs. 2a Satz 2 SächsPVDG-E) sollte in der Wendung „wenn im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr“ u. E. das Wort „auch“ entfallen.

8. In Nummer 26 (§ 79c Abs. 2 Satz 3 SächsPVDG-E) heißt es:

„Kann der Zweck des Tests oder Trainings mit pseudonymisierten Daten nicht erreicht werden oder ist die Pseudonymisierung nur mit unverhältnismäßigem Aufwand möglich, dürfen personenbezogene Daten zum Zweck des Tests oder Trainings verarbeitet werden.“

Das sehen wir kritisch. U. E. sollte es heißen:

„...dürfen personenbezogene Daten zum Zweck des Tests oder Trainings nicht verarbeitet werden.“

Anderenfalls kann nicht sichergestellt werden, dass nicht pseudonymisierte personenbezogene Daten beim Auftragsverarbeiter nicht missbräuchlich verwendet werden (können). Die Regelungen in Absatz 5 scheinen uns eher nicht ausreichend und sie verhalten sich auch nicht zu nicht pseudonymisierten Daten.

9. Soweit es in Nummer 30 (§ 88 Abs. 1 SächsPVDG-E) heißt „... denen ein privilegierter Zugang ...“ bleibt, auch nach der Begründung (S. 108), offen, was mit dem Begriff des privilegierten Zugangs gemeint ist. Der Begriff sollte präzisiert werden, etwa dahin, dass mit ihm nur Bedienstete eines Veranstalters gemeint sind oder - wenn das zutrifft - möglicherweise auch „privilegierte Besucher“. Jedenfalls sollte der in der Begründung verwendete Begriff der „Nähe“ zumindest dort näher konkretisiert werden.

10. Mit Artikel 2 Nummer 1 (§ 23 Abs. 2 SächsPBG-E) wird die Entscheidung des Bundesverfassungsgerichts vom 12. März 2019 - 2 BvR 675/14 - (Rn. 66) über die Bestimmung der Nachtzeit durch einen Verweis auf § 104 Abs. 3 StPO umgesetzt. Das ist nicht zu beanstanden.

11. Mit Artikel 2 Nummer 2 (§ 30 Abs. 1 SächsPBG-E) wird das Urteil des Verfassungsgerichtshofs v. 25. Januar 2024 - Vf. 91-II-19 - im Hinblick auf die Bestimmung des Anlasses, des Zwecks und der Grenzen der Datenerhebung durch den Einsatz technischer

Mittel zur Bildaufnahme und -aufzeichnung in öffentlich zugänglichen Räumen (Tenor Ziffer 5 der Entscheidung) umgesetzt. Diese Umsetzung erscheint uns hinreichend.

12. Es sollte geprüft werden, ob nicht ein Artikel zum Zitiergebot aufzunehmen ist. Das Änderungsgesetz enthält selbst Grundrechtseinschränkungen, die von § 10 SächsPVDG und § 10 SächsPBG nicht abgedeckt sind. Daher dürfte erneut ein gesetzlicher Hinweis auf Grundrechtseinschränkungen erforderlich sein. Dieser Hinweis sollte in einem der Schlussartikel des Änderungsgesetzes aufgenommen werden (vgl. Handbuch der Rechtsförmlichkeit, 4. Aufl., Rn. 557).

Für Rückfragen und Erörterungen stehen wir gern zur Verfügung.

Mit freundlichen Grüßen



Dr. Matthias Mittag
Verbandsvorsitzender

Sächsisches Staatsministerium des Innern
01095 Dresden

Dresden, 25.11.2025

Stellungnahme zur Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG)

Sehr geehrte Damen und Herren,

wir bedanken uns zur Möglichkeit der Stellungnahme zur Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG).

Zum vorliegenden Entwurf haben wir keine weiteren Anmerkungen. Wir begrüßen die dort enthaltenen Änderungen. Dies trägt dazu bei die Sächsische Polizei gezielt zu stärken, um auf aktuelle und künftige Herausforderungen angemessen reagieren zu können und unterstützt somit auch die Feuerwehren und Hilfsorganisationen in der Durchführung ihrer hoheitlichen Aufgaben nach SächsBRKG.

Mit freundlichen Grüßen



Gunnar Ullmann

Präsident

VSW • Bautzner Straße 17 • 01099 Dresden

per E-Mail an:
Anhoerung.SaechsPVDG@smi.sachsen.de

Dresden, 01.12.2025
ma-büh

Novellierung des Polizeivollzugsdienstgesetzes (SächsPVDG)
Anhörung des Referentenentwurfs
Stellungnahme der Vereinigung der Sächsischen Wirtschaft e. V. (VSW)

Sehr geehrte Damen und Herren,

namens und im Auftrag der VSW bedanken wir uns für die Gelegenheit, im Rahmen der Anhörung zum Entwurf des Polizeivollzugsdienstgesetzes (SächsPVDG) unsere Perspektive einzubringen.

Wir begrüßen sehr, dass der vorliegende Gesetzentwurf verfassungskonform das Polizeirecht des Freistaates Sachsen auf eine moderne, technisch aktuelle Basis stellen will. Der Gesetzentwurf greift die Herausforderungen unserer Zeit auf und wappnet die Polizei, den Aufgaben zum Erhalt der öffentlichen Sicherheit genüge leisten zu können. Die vorgesehene Ausgestaltung der Befugnisse und Kompetenzen entspricht dem Niveau, das inzwischen in zahlreichen anderen Bundesländern gilt, die bereits ihre Polizeigesetze angepasst haben oder sich aktuell in Anpassungsprozessen befinden. Aus unserer Sicht müssen der Polizei im Freistaat Sachsen die notwendigen Befugnisse eingeräumt werden, um die Bevölkerung und Unternehmen wirksam vor Straftaten schützen zu können.

Besonders positiv zu bewerten sind folgende Aspekte:

- Die Erweiterung der Befugnisse zur Abwehr gefährlicher Drohnen sowie der Einsatz von Drohnen zur Lageerkundung.
- Die Einführung von Distanz-Elektroimpulsgeräten (Taser) als wichtiges Instrument zur Deeskalation.
- Die Ausweitung des Einsatzes von Bodycams auf Wohn- und Geschäftsräume außerhalb der Öffnungszeiten, um Einsatzkräfte in kritischen Situationen besser zu schützen, Klarheit durch Aufnahmen zu schaffen und falschen Darstellungen vorzubeugen.

- Die Anwendung moderner IT-Systeme zur automatisierten Datenanalyse, beispielsweise bei der Bekämpfung von Terrornetzwerken, um den wachsenden Datenmengen im digitalen Zeitalter gerecht zu werden.
- Die Ermöglichung des verdeckten Einsatzes der automatisierten Kennzeichenerkennung zur unauffälligen Identifikation gesuchter Fahrzeuge.
- Der Einsatz intelligenter Videoüberwachung an Kriminalitätsschwerpunkten, um Gefahren im öffentlichen Raum frühzeitig zu erkennen und die Bevölkerung besser zu schützen.
- Die rechtlich geregelte Anwendung der Quellen-Telekommunikations-Überwachung (Quellen-TKÜ) unter richterlicher Kontrolle, damit die Sicherheitsbehörden auch im digitalen Raum handlungsfähig bleiben.
- Die Nutzung öffentlich zugänglicher Daten im anlassbezogenen Abgleich zur gezielten Fahndung nach schweren Straftätern und Terrorgefährdern, um Fahndungserfolge zu steigern.

Mit dem Gesetzentwurf wird nicht nur ein modernes Instrumentarium für die sächsische Polizei geschaffen, sondern zugleich ein bedeutender Schritt zur Erhöhung der Sicherheit und des Schutzes der Bevölkerung im Freistaat Sachsen getan.

Damit trägt der Entwurf maßgeblich dazu bei, die Polizei für die Herausforderungen der Gegenwart und Zukunft auszustatten und damit einen nachhaltigen Beitrag zur öffentlichen Sicherheit zu leisten.

Mit freundlichen Grüßen


Dr. Jörg Brückner
Präsident


Matthias Matz
Hauptgeschäftsführer



Landesverkehrswacht Sachsen e.V. - Kesselsdorfer Straße 336 b
01156 Dresden

Peggy Frey
stv. Referatsleiterin
Referat Recht der Polizei

Gemäß Verteiler
Ausschließlich per E-Mail

Schirmherrin -
Sächsische Staatsministerin für
Infrastruktur und Landesentwicklung

Landesverkehrswacht Sachsen e.V.
Telefon: +49 351 5633030
www.lvw-sachsen.de
info@lvw-sachsen.de

Dresden, 14.11.2025

**Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG);
Anhörung des Referentenentwurfes**

Stellungnahme der Landesverkehrswacht Sachsen e.V.

Die Landesverkehrswacht Sachsen e.V. (LVW) ist mit ihren 24 örtlichen Verkehrswachten (OVW) und ca. 1.000 Mitgliedern seit 35 Jahren eine der ältesten Bürgerinitiativen für Verkehrssicherheit im Freistaat Sachsen. Unsere satzungsgemäße Aufgabe ist die Unfallverhütung, um die Sicherheit auf Sachsens Straßen zu erhöhen und somit die Zahl der Unfälle zu reduzieren. Dazu bieten wir ein breites Angebot an Maßnahmen zur Verkehrserziehung und -aufklärung in allen Alters- und Zielgruppen.

Die Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG) ist ein Erfordernis der aktuellen Entwicklung in der Gesellschaft mit Regelungen, die auch unsere ehrenamtlichen Mitglieder und hauptamtlichen Mitarbeiter bei öffentlichen Veranstaltungen schützen. Die Befugnisse der Polizei dazu finden wir zweckmäßig und ausgewogen.

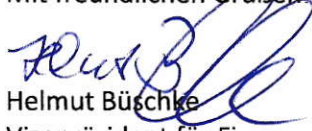
Im öffentlichen Verkehrsraum ist es auch nach unserer Ansicht notwendig, Aufzeichnungen und Videoüberwachungen durchzuführen, um Ereignisse aufklären zu können.

Für die Verhütung von Ordnungswidrigkeiten und Straftaten kommen notwendige und ausgewogene Maßnahmen der Polizei zur Anwendung. Die Datenerfassung und Auswertung zum Schutz von Bürgern und Sachen sehen wir als notwendig an. Die Regelungen sind generell geeignet, um eine gute Polizeiarbeit zu leisten.

Besonders die neuen Regelungen zur Einhaltung der Verkehrsvorschriften durch moderne Überwachungstechniken werden helfen, Unfälle zu vermeiden und besser aufzuklären. Die klar geregelten Befugnisse sichern eine höhere Qualität der polizeilichen Arbeit. Die präventive Überwachung von Fahrzeugen in Straßenverkehr ist für die Vermeidung von Verkehrsunfällen notwendig.

Wünschen würden wir uns mehr Prävention in den Schulen zum verkehrsgerechten Verhalten im Straßenverkehr.

Mit freundlichen Grüßen



Helmut Büschke
Vizepräsident für Finanzen

Von: [Fachstelle Gewaltfreies Zuhause](#)
An: [Frey, Peggy \(SMI\)](#); [SMI Anhörung SächsPVDG](#)
Cc: [Annabell Pfützner](#); [Kevin Idel](#); [Stefanie Thieroff](#); [Eva-Maria Hoffmann](#)
Datum: Montag, 17. November 2025 10:57:17

Sehr geehrte Frau Frey,

bei der LKA-Opferschutztagung vergangene Woche haben wir erfahren, dass ausschließliche die Opferhilfe Sachsen e.V. zu einer Stellungnahme bzgl. der Novellierung SächsPVDG angeschrieben wurde.

Wir bedauern, dass die LAG Gewaltfreies Zuhause Sachsen e.V. mit seiner umfassenden Expertise nicht beteiligt wurde und möchten an dieser Stelle unsere Zuarbeit mit Bitte um Berücksichtigung senden:

Thema Weitergabe der Daten des Gewaltausübenden, Notwendigkeit zur Ergänzung dieses Themenbereiches in **Â§ 84**:

Mehrere Bundesländer haben die Weitergabe solcher Daten bereits gesetzlich etabliert, unter anderem Schleswig-Holstein mit dem **Gesetz zum besseren Schutz von Opfern häuslicher Gewalt und bei Nachstellungen durch den Einsatz der elektronischen Aufenthaltsüberwachung und weitere Änderungen des Landesverwaltungsgesetzes** (vom 26. März 2025, GVOBl. Schl.-H. 2025/51 vom 14. April 2025). Dort heißt es in **Â§ 201a Absatz 6**:

„Unbeschadet ihrer Mitteilungspflichten nach anderen Vorschriften hat die Polizei unter den Voraussetzungen von Absatz 1 und 2 die für eine Kontaktaufnahme erforderlichen personenbezogenen Daten wie folgt an Beratungsstellen zu übermitteln:

1. die Daten der gefährdeten Person an eine geeignete Beratungsstelle zum Schutz vor häuslicher Gewalt;
2. die Daten der Person, von der die Gefahr ausgeht, an eine geeignete Beratungsstelle für gewaltausübende Menschen;
3. sofern eine minderjährige Person im Haushalt der gefährdeten Person lebt, die Daten der gefährdeten Person und der minderjährigen Person an eine auf die Belange von Kindern oder Jugendlichen ausgerichtete, geeignete Beratungsstelle.“

Diese Regelung zeigt, dass die datenschutzkonforme Weitergabe von Informationen an Täterberatungsstellen ein wirksames und rechtlich abgesichertes Instrument zur frühzeitigen Intervention und Prävention häuslicher Gewalt darstellen kann. Weiter ist es nicht ersichtlich, warum es kein Datenschutzproblem ist, dass die Daten der Betroffenen weitergegeben werden können, aber nicht der Gewaltausübenden.

Es ist daher notwendig, dass **Â§ 84 ergänzt wird, Vorschlag:**

Zum Zweck der Bekämpfung häuslicher Gewalt können neben den Daten der von Gewalt betroffenen Personen auch die relevanten personenbezogenen Daten der Gewalt ausübenden Person an die anerkannten Täterberatungsstellen übermittelt werden. Die Übermittlung erfolgt ausschließlich zum Zweck, den Kontakt zur Gewalt

ausreichenden Person herzustellen und diese über die Möglichkeit einer freiwilligen Beratung und Unterstützung in spezialisierten Einrichtungen für Gewaltausübende zu informieren. Die Täterberatungsstellen dürfen die ermittelten Daten nur für diesen Zweck verwenden und sind verpflichtet, den Datenschutz gemäß den geltenden gesetzlichen Bestimmungen sicherzustellen.

Mit freundlichen Grüßen

i.A.

Lisa Rechenberg

Fachstelle Häusliche Gewalt der LAG gewaltfreies Zuhause Sachsen e.V.



Tel.: 0351 20 66 10 42

Lisa Rechenberg (Pronomen sie/ihr); Mobil: +49152 2174 8865

Teresa Golschewski (Pronomen sie/ihr); Mobil: +49152 2174 8777

www.gewaltfreieszuhause.info

Spendenkonto - Ihre Spende für den Gewaltschutz in Sachsen unter dem Stichpunkt "Spende" an: DE07 4306 0967 1242 8194 00

Von: [GP Bw LKdo SN stvKdr und ChdSt](#)
An: [SMI Anhörung SächsPVDG](#)
Cc: [GP Bw LKdo SN stvKdr und ChdSt](#); [GP Bw LKdo SN Kommandeur](#)
Datum: Dienstag, 18. November 2025 15:19:02
Anlagen: [image001.jpg](#)
[image002.png](#)
[image003.jpg](#)

OFFEN \ PersDat Schutzbereich 1

Landeskommando Sachsen Chef des Stabes



Stellungnahme Landeskommando Sachsen:

Die Bundeswehr ist Träger der militärischen Verteidigung. Die Landes- und Bundeswehrverteidigung ist dabei Kernauftrag der Bundeswehr.

Militärische und zivile Infrastrukturen im Freistaat Sachsen zur Unterstützung von Verlegungen verbündeter und eigener Streitkräfte sowie die mit Verlegungen im Zusammenhang stehenden organisatorischen Maßnahmen für alle Verkehrsarten sind deshalb soweit vorzubereiten und zu ertüchtigen, dass sie

- (1) die Verlegung zeitgerecht unterstützen können,
- (2) die Rolle Deutschlands als „Drehscheibe“ ermöglichen und so
- (3) die Bewegungs- und Handlungsfreiheit im Rahmen der Bundes- und Landesverteidigung gewährleisten.

Im Rahmen der Inneren Sicherheit leisten die Polizeien der Bundesländer und die Bundespolizei dazu einen unverzichtbaren Beitrag.

Der Flug von Drohnen kann (1) Flugverbotszone verletzen, (2) auf Ausspähungen oder (3) einen Angriff hindeuten. Somit kann der Einsatz von Drohnen eine rechtswidrige Störung oder eine Straftat darstellen. Das erfordert entsprechende Gegenmaßnahmen. Der Einsatz eigener Drohnen kann einen Beitrag zur Informationsbeschaffung und zur Verdichtung des Lagebildes leisten und ist in der Bundeswehr seit Jahrzehnten gängige Praxis.

In dem Bewusstsein, dass äußere und innere Sicherheit weniger zu trennen sind, ist aus hiesiger Sicht die entsprechende Gestaltung der Kompetenzen und Befugnisse der Landespolizei im Freistaat Sachsen geboten.

Im Auftrag

Markus Kankleit
Oberstleutnant



Landeskommando Sachsen
stv. Kommandeur und Chef des Stabes

Marienallee 14 | D 01099 Dresden



Telefon: +49 (0) 351 823-4202 (Bw: 8910)

E-Mail: LKdoSNstvKdrundCHdSt@bundeswehr.org

Internet: <http://www.bundeswehr.de>

Von: [Post - SBB Dresden](#)
An: [SMI Anhörung SächsPVDG](#)
Datum: Donnerstag, 13. November 2025 15:09:05
Anlagen: [image003.jpg](#)
[Stellungnahme DPolG zum SächsPVDG 30.10.2025.pdf](#)

Sehr geehrte Damen und Herren,

vielen Dank für die Möglichkeit zur Stellungnahme zur geplanten Novellierung des Sächsischen Polizeivollzugsdienstgesetzes.

Anbei übersenden wir Ihnen die Stellungnahme unserer Mitgliedsgewerkschaft DPolG Deutsche Polizeigewerkschaft, Landesverband Sachsen e.V., der wir uns inhaltlich anschließen.

An dieser Stelle möchten wir ausdrücklich darauf hinweisen, dass die geplanten Maßnahmen zwingend einer entsprechenden Bereitstellung ausreichender finanzieller Mittel bedürfen.

Mit freundlichen Grüßen
Nannette Seidler

Anhang



Landesvorsitzende
Theresienstraße 15
01097 Dresden
Telefon: 0351-47 16 824
E-Mail: post@sbb.dbb.de
Internet: www.sbb.de
Facebook: SBB Beamtenbund und Tarifunion Sachsen
Insta: [sbb_dbb_sachsen](#)

Opferhilfe Sachsen e. V. - Heinrichstraße 12 - 01097 Dresden

Sächsisches Staatsministerium des Innern

01095 Dresden

Dresden, 14. November 2025

Betreff: Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG); Anhörung des Referentenentwurfes (Geschäftszeichen: 36-2002/25/14)

Sehr geehrte Damen und Herren,

als Vertreter des Opferhilfe Sachsen e.V. bedanke ich mich für die Gelegenheit, zum Referentenentwurf des Sächsischen Polizeivollzugsdienstgesetzes Stellung nehmen zu dürfen.

Unsere Mitarbeitenden in den Fachberatungsstellen arbeiten seit fast drei Jahrzehnten sehr vertrauensvoll und konstruktiv mit der Sächsischen Polizei zusammen, um Betroffenen von Straftaten durch psychosoziale Beratung und Begleitung Hilfe und Unterstützung geben zu können und präventiv Menschen vor Straftaten zu schützen. Dabei kommen Menschen zu uns, die verschiedene Straftaten, vor allem Gewaltstraftaten, erlebt haben; unter anderem auch aus dem Bereich Häuslicher Gewalt und Stalking. Gerade bei diesen Delikten arbeiten wir im Netzwerk mit den Interventionsstellen gegen Häusliche Gewalt eng zusammen. Anders als in unserer Struktur können die Kolleginnen in diesen Beratungsstellen proaktiv auf die Betroffenen zugehen. Das ist im § 84 SächsPVDG geregelt und wir sehen es im Interesse eines ganzheitlichen Ansatzes, Menschen vor weiterer Gewalt zu schützen als wichtige Ergänzung zu unserer Komm-Struktur an.

Aus Sicht eines erweiterten und aktiven Opferschutzes und damit zusammenhängend im Interesse einer frühzeitigen Intervention und Prävention von Gewaltstraftaten sind wir daher ausdrücklich dafür, dass Täterberatungsstellen ebenfalls proaktiv auf gewaltausübende Personen zugehen können. Deshalb befürworten wir, dass die dafür notwendige Datenweitergabe durch die Polizei nach gleichen datenschutzrechtlichen Maßgaben wie bei gewaltbetroffenen Personen in den § 84 SächsPVDG aufgenommen werden sollte.

Mit freundlichen Grüßen



Andreas Edhofer (Geschäftsführer)

Geschäftsstelle

Opferhilfe Sachsen e. V.
Geschäftsstelle
Heinrichstraße 12
01097 Dresden

Telefon: 0351 / 811 38 98
Fax: 0351 / 810 81 91
gfma@opferhilfe-sachsen.de
www.opferhilfe-sachsen.de

Vereinsregister

Reg.-Nr. VR 2951 beim
Amtsgericht Dresden
Finanzamt Dresden-Nord
Steuer-Nr.: 202/141/06125

Spendenkonto

Opferhilfe Sachsen e. V.
Commerzbank AG
BIC: COBADEFFXXX
IBAN: DE22 8704 0000 0601 4252 01



DPoIG

Deutsche Polizeigewerkschaft im dbb
Landesverband Sachsen e.V.

Sächsisches Staatsministerium des Innern

01095 Dresden

Landesgeschäftsstelle

Theresienstr. 15

01097 Dresden

Tel.: 0351 / 471 68 28

Fax: 0351/ 811 36 84

Dresden, 30.10.2025

Stellungnahme zum Referentenentwurf der Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG) vom 02.10.2025

Die Deutsche Polizeigewerkschaft e. V. (DPoIG) begrüßt ausdrücklich die geplante Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG) im Lichte des Urteils des Sächsischen Verfassungsgerichtshofs vom 25. Januar 2024. Der Gesetzgeber hat damit die Gelegenheit, die bestehenden Regelungen nicht nur an die verfassungsgerichtlichen Anforderungen anzupassen, sondern zugleich ein modernes, zukunftsfähiges und praxistaugliches Polizeigesetz zu schaffen. Dabei ist entscheidend, dass der Gesetzgeber die notwendige Balance zwischen effektiver Gefahrenabwehr und dem Schutz der Grundrechte wahrt.

Verfassungsgerichtliche Maßstäbe und gesetzgeberische Zielsetzung

Das Urteil des Sächsischen Verfassungsgerichtshofs (Vf. 91 II 19) verdeutlichte, dass polizeiliche Eingriffe klaren rechtlichen Grenzen unterliegen müssen und dass Datenerhebungs- und Überwachungsmaßnahmen nur auf präzise, normenklar formulierte Ermächtigungsgrundlagen gestützt werden dürfen. Der vorliegende Gesetzentwurf 2025 setzt diese Maßstäbe in wesentlichen Punkten um, indem er etwa Evaluationspflichten (§ 61 Abs. 7 SächsPVDG), richterliche Vorbehalte und Kontrollmechanismen bei verdeckten Maßnahmen vorsieht. Die DPoIG erkennt diese Schritte an, betont jedoch, dass gesetzliche Klarstellungen nicht zu einer faktischen Einschränkung polizeilicher Handlungsmöglichkeiten führen dürfen. Rechtssicherheit muss mit praktischer Wirksamkeit einhergehen.

Bewertung zentraler Regelungsinhalte

1. Verwendung des Begriffs der „Vorfeldstraftat“ (§ 4 Nr. 6 SächsPVDG)

Die Aufnahme des Begriffs „Vorfeldstraftat“ ist aus polizeifachlicher Sicht nachvollziehbar, da sie eine frühzeitige Gefahrenabwehr bei drohenden schweren Straftaten ermöglichen soll.

Amtsgericht Dresden

VR-Nr. 2555
Sitz des Vereins: Dresden

Geschäftsführender Landesvorstand:

Cathleen Martin (Landesvorsitzende)
Toni Starke (Stellvertreter)
Maik Ebersbach (Stellvertreter)
Elisabeth Capelle (Stellvertreterin)

Bankverbindung:

BBBank Karlsruhe
Kto.-Nr.: 877 20 37
Blz.: 660 908 00

Allerdings ist die derzeitige Definition zu weit gefasst. Es besteht die Gefahr, dass Handlungen unter diese Kategorie fallen, die keine objektiv überprüfbaren Hinweise auf eine erhebliche Gefahr liefern. Dies widerspräche dem Bestimmtheitsgrundsatz. Die DPolG fordert daher eine klarstellende Einschränkung des Begriffs auf strafbare Vorbereitungshandlungen nach §§ 89a, 89b, 129a StGB. Nur so bleibt die Norm mit der Rechtsprechung des Bundesverfassungsgerichts und des SächsVerfGH vereinbar.

Zugleich betont die DPolG, dass eine wirksame Prävention terroristischer und extremistischer Gewalt ohne ein Eingreifen im Vorfeld nicht möglich ist. Die Norm muss daher so formuliert werden, dass die Polizei im Fall konkreter Anhaltspunkte tätig werden kann, ohne auf eine unmittelbar bevorstehende Tat warten zu müssen.

2. Tatbestandsmerkmal der „öffentlichen Ordnung“ (§ 18 SächsPVDG)

Die Wiederaufnahme des Begriffs der „öffentlichen Ordnung“ ist aus Sicht der DPolG zu begrüßen. Die bisherige Beschränkung auf die „öffentliche Sicherheit“ führte zu erheblichen Vollzugsproblemen, da viele Lagen nicht von der polizeilichen Eingriffsbefugnis erfasst wurden, obwohl sie das friedliche Zusammenleben erheblich beeinträchtigten.

Der Begriff der öffentlichen Ordnung ist verfassungsrechtlich unbedenklich, wenn er – wie im Entwurf vorgesehen – durch den Verhältnismäßigkeitsgrundsatz begrenzt wird. In der Praxis betrifft dies etwa Lagen bei aggressivem Betteln, extremen Ruhestörungen oder einschüchternden Auftritten extremistischer Gruppierungen. Die DPolG fordert daher ausdrücklich, den Begriff der öffentlichen Ordnung als eigenständiges Schutzgut beizubehalten und in der Gesetzesbegründung praxisnah zu konkretisieren, um die Rechtssicherheit der handelnden Beamtinnen und Beamten zu stärken.

3. Bewertung des § 57a SächsPVDG – Automatisierte Verarbeitung offen erhobener personenbezogener Daten

§ 57a SächsPVDG ist ein zentraler Bestandteil des Gesetzentwurfs. Er reagiert auf die technologische Entwicklung, wonach moderne Datenverarbeitung auch im öffentlichen Raum eine immer größere Rolle spielt. Die DPolG unterstützt grundsätzlich die Einführung dieser Vorschrift, da sie eine rechtsklare Grundlage für die Nutzung digitaler Systeme, wie Gesichtserkennung oder Musteranalyse, schafft. Weiterhin sieht die DPolG Sachsen dabei keinen Hinweis auf eine anlasslose Massenüberwachung.

Die DPolG fordert daher:

- Eine eindeutige Zweckbindung (z. B. Terrorismus, schwere Gewalt- oder Sexualdelikte).
- Eine richterliche Anordnungspflicht bei biometrischen Echtzeiterkennungen.
- Eine regelmäßige Evaluierung und technische Zertifizierung der eingesetzten Systeme. Damit kann der notwendige Ausgleich zwischen Bürgerrechten und Sicherheit erreicht werden.

4. Drittbetroffenheit (§ 66 Abs. 2a Nr. 4 und 5 SächsPVDG)

Die Vorschrift des § 66 Abs. 2a SächsPVDG befasst sich mit den Rechten Dritter, deren Daten im Rahmen verdeckter Überwachungsmaßnahmen miterfasst werden. Die DPolG erkennt den

Amtsgericht Dresden

VR-Nr. 2555
Sitz des Vereins: Dresden

Geschäftsführender Landesvorstand:

Cathleen Martin (Landesvorsitzende)
Toni Starke (Stellvertreter)
Maik Ebersbach (Stellvertreter)
Elisabeth Capelle (Stellvertreterin)

Bankverbindung:

BBBank Karlsruhe
Kto.-Nr.: 877 20 37
Blz.: 660 908 00

Schutz unbeteiligter Personen als verfassungsrechtlich geboten an, weist jedoch darauf hin, dass eine übermäßige Formalisierung der Lösch- und Dokumentationspflichten die Einsatzpraxis erheblich erschweren würde. Eine zu enge Handhabung könnte etwa bei der Telekommunikationsüberwachung oder der Online-Durchsuchung dazu führen, dass wertvolle Erkenntnisse verloren gehen. Die DPolG fordert daher, die Löschpflichten technisch und organisatorisch so auszugestalten, dass sie praktikabel bleiben. Zugleich sollte der Gesetzgeber klarstellen, dass die Polizei Daten Dritter temporär speichern darf, wenn deren Auswertung für die Beurteilung der Hauptmaßnahme notwendig ist. Damit wird ein verhältnismäßiger Ausgleich zwischen Datenschutz und Sicherheit geschaffen.

Konkrete Änderungs- und Präzisierungsvorschläge

Die DPolG regt folgende gezielte Änderungen des Gesetzentwurfs an, um Rechtsklarheit, Praktikabilität und Gleichlauf mit bestehenden Regelungen des Polizeirechts sicherzustellen:

a) Definition des Kontaktverbots (§ 19 Abs. 1 SächsPVDG)

Die Regelung zum Kontaktverbot bedarf einer inhaltlichen Konkretisierung. Aus Sicht der DPolG sollte gesetzlich festgeschrieben werden, dass ein Kontaktverbot jede Form direkter oder indirekter Kommunikation umfasst – einschließlich persönlicher, schriftlicher, telefonischer und digitaler (z. B. über soziale Netzwerke oder Messenger-Dienste) Kontakte. Zudem sollte klargestellt werden, dass das Verbot auch die mittelbare Kontaktaufnahme über Dritte erfasst.

Eine solche Präzisierung schafft Klarheit für die betroffenen Personen und für die Polizei, die über die Einhaltung zu wachen hat. Mithin sollte der Begriff des Kontaktverbotes in den § 4 SächsPVDG – Begriffsbestimmungen aufgenommen und dort, wie oben beschrieben definiert werden.

b) Änderung des § 22 Abs. 1 Nr. 2 SächsPVDG

Die DPolG empfiehlt, das Wort „*Straftat*“ durch „*rechtswidrige Tat*“ zu ersetzen. Diese Formulierung entspricht der Regelungssystematik der §§ 16 und 44 SächsPVDG und trägt der Tatsache Rechnung, dass auch Personen, die strafunmündig sind (insbesondere Kinder unter 14 Jahren, psychisch Kranke), durch polizeiliche Maßnahmen in Obhut oder Gewahrsam genommen werden können, wenn sie eine erhebliche Gefahr verursachen oder sich selbst gefährden.

Die Anpassung ist erforderlich, um einen einheitlichen Sprachgebrauch im Gesetz sicherzustellen und unbeabsichtigte Schutzlücken zu vermeiden.

c) Klarstellung des Zeitbezugs in § 26 Abs. 1 Nr. 3 SächsPVDG

Im Entwurf bleibt unbestimmt, welcher „Tag“ bei der Fristberechnung maßgeblich ist. Zur Vermeidung von Auslegungsschwierigkeiten sollte der Wortlaut analog zu § 22 Abs. 7 Satz 4 SächsPolG a. F. gefasst werden, wonach der Tag des Beginns der Freiheitsentziehung nicht mitzählt.

Diese Klarstellung stellt sicher, dass Fristen eindeutig berechnet werden und Betroffene wie Behörden gleichermaßen Rechtssicherheit haben.

d) Ergänzung des § 29 Abs. 3 Satz 1 SächsPVDG

Amtsgericht Dresden

VR-Nr. 2555
Sitz des Vereins: Dresden

Geschäftsführender Landesvorstand:

Cathleen Martin (Landesvorsitzende)
Toni Starke (Stellvertreter)
Maik Ebersbach (Stellvertreter)
Elisabeth Capelle (Stellvertreterin)

Bankverbindung:

BBBank Karlsruhe
Kto.-Nr.: 877 20 37
Blz.: 660 908 00

Nach geltendem Entwurf sind Durchsuchungen zur Nachtzeit grundsätzlich unzulässig, es sei denn, sie erfolgen in den in § 29 Abs. 1 Satz 1 Nr. 2 genannten Fällen.

Die DPolG hält es für erforderlich, auch die Nummer 1 (also Fälle wenn Tatsachen die Annahme rechtfertigen, dass sich in ihr eine Person befindet, die in Gewahrsam genommen werden darf) in den Ausnahmekatalog aufzunehmen.

Nur so wird sichergestellt, dass polizeiliches Einschreiten bei dringenden Gefahrenlagen – etwa bei Vermisstenfällen oder akuter Gefährdung von Opfern häuslicher Gewalt – rechtssicher möglich bleibt.

Die Ergänzung dient damit dem Schutz der Bevölkerung und der Rechtssicherheit der eingesetzten Kräfte.

e) Präzisierung des § 41 Abs. 2 SächsPVDG

§ 41 Abs. 2 SächsPVDG verweist derzeit auf § 57 Abs. 4 SächsPVDG, der lediglich die technische Funktion des sogenannten *Prerecordings* (Voraufzeichnung) beschreibt. Die Intention des Gesetzgebers besteht jedoch darin, den gesamten Einsatz unmittelbaren Zwangs zu erfassen – also nicht nur die sechzigsekündige Vorphase, sondern die gesamte Maßnahme. Die DPolG schlägt daher vor, den Verweis auf § 57 **Abs. 4** zu streichen und stattdessen klarzustellen, dass der Einsatz der Bodycam in allen Phasen unmittelbaren Zwangs rechtlich zulässig und technisch abzusichern ist. Diese Präzisierung dient der Eindeutigkeit der Vorschrift und der Rechtssicherheit für Einsatzkräfte.

f) Implementierung des proaktiven Täteransatzes ins SächsPVDG

Der proaktive Täteransatz bedeutet, dass polizeiliche Befugnisse nicht erst bei konkreter Gefahr oder begründetem Verdacht ansetzen, sofern bereits zur Früherkennung möglicher Täter eingesetzt werden können – also zur antizipativen Identifikation potentieller Täter.

Ziel soll sein, dass eine frühzeitige Identifikation und Beobachtung von Personen, die möglicherweise künftig erhebliche Straftaten begehen können stattfindet. Der dazu im Gegensatz stehende reaktive Ansatz ist bereits im Entwurf des § 84 SächsPVDG verankert.

Jedoch erfordert ein solcher Ansatz klare gesetzliche Tatbestandsvoraussetzungen, um Willkür und Grundrechtsverstößen zu verhindern. Es braucht eine enge Zweckbindung (z. B. Schutz hochrangiger Rechtsgüter), sowie eine richterliche Kontrolle oder behördliche Genehmigungspflichten.

Die DPolG Sachsen schlägt deshalb vor, die Regelung des proaktiven Täteransatzes ins SächsPVDG aufzunehmen. Nach Möglichkeit sollte dies als neuzufassenden § 84a – Proaktive Datenübermittlung zur Früherkennung von Gefahrenpersonen geschehen.

Amtsgericht Dresden

VR-Nr. 2555
Sitz des Vereins: Dresden

Geschäftsführender Landesvorstand:

Cathleen Martin (Landesvorsitzende)
Toni Starke (Stellvertreter)
Maik Ebersbach (Stellvertreter)
Elisabeth Capelle (Stellvertreterin)

Bankverbindung:

BBBank Karlsruhe
Kto.-Nr.: 877 20 37
Blz.: 660 908 00

Schlussbemerkung

Die DPolG sieht im Gesetzentwurf 2025 einen wichtigen Schritt zu einem modernen und rechtssicheren Polizeirecht in Sachsen. Entscheidend wird sein, dass der Landtag die genannten Punkte – insbesondere die Präzisierung des Begriffs „Vorfeldstraftat“, die Klarstellung des § 57a sowie die praktikable Ausgestaltung des § 66 Abs. 2a – aufgreift.

Nur so kann gewährleistet werden, dass die Polizei ihre Aufgaben im Sinne der Sicherheit der Bürgerinnen und Bürger effektiv erfüllen kann. Die Deutsche Polizeigewerkschaft e. V. erklärt ihre Bereitschaft, den Gesetzgebungsprozess weiterhin aktiv und konstruktiv zu begleiten.

Mit freundlichen Grüßen



Maik Ebersbach

stellv. Landesvorsitzender DPolG Sachsen e. V.

Amtsgericht Dresden

VR-Nr. 2555
Sitz des Vereins: Dresden

Geschäftsführender Landesvorstand:

Cathleen Martin (Landesvorsitzende)
Toni Starke (Stellvertreter)
Maik Ebersbach (Stellvertreter)
Elisabeth Capelle (Stellvertreterin)

Bankverbindung:

BBBank Karlsruhe
Kto.-Nr.: 877 20 37
Blz.: 660 908 00



**Gewerkschaft
der Polizei**
Sachsen

Gewerkschaft der Polizei • Sachsenallee 16 • 01723 Kesselsdorf

Sächsisches Staatsministerium des Innern
Abt. 3 – Landespolizeipräsidium
Ref. 36

per Mail an
Anhoerung.saechsPVDG@SMI.sachsen.de

**Sachsenallee 16
01723 Kesselsdorf**

Tel.: 03 52 04/6 87 11
Fax: 03 52 04/6 87 50

gdp@gdp-sachsen.de
www.gdp-sachsen.de
Steuernummer: 210/142/17557

14.11.2025
AS-JK

Stellungnahme zum Referentenentwurf des Gesetzes zur Änderung polizeirechtlicher Vorschriften

Sehr geehrte Damen und Herren,

wird danken für die Möglichkeit zur Stellungnahme und beziehen als Gewerkschaft der Polizei, Landesbezirk Sachsen e. V. (GdP Sachsen) zum o. g. Entwurf in Bezug auf Artikel 1 wie folgt Stellung:

I. Vorbemerkung

In einer sich ständig verändernden Welt mit ihren multiplen Bedrohungs- und Gefährdungslagen ist es von großer Bedeutung, dass die Polizei über ein modernes, zukunftsfähiges und rechtssicheres Polizeigesetz verfügt. Nur so kann sie ihren Aufgaben zum Schutz der Bürgerinnen und Bürger wirksam und im Einklang mit den Grundrechten nachkommen.

Neben den Anpassungen aufgrund höchstrichterlicher Entscheidungen ist ein wesentlicher Grund für die Notwendigkeit der Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG) die Anpassung an diese neue Sicherheitslagen. Die Bedrohungen unserer Zeit unterscheiden sich deutlich von denen früherer Jahrzehnte. Cyberkriminalität, Terrorismus oder organisierte Kriminalität stellen ganz neue Herausforderungen dar, auf die die sächsische Polizei angemessen reagieren muss. Ein veraltetes Gesetz reicht dafür auch mit Hinblick auf die steigenden Fallzahlen, die neuen Kriminalitätsphänomene und den stark begrenzten Personalbestand nicht mehr aus.

Zudem entwickeln sich die technischen Möglichkeiten rasant weiter. Kriminelle nutzen moderne Technologien, agieren über das Internet, nutzen Verschlüsselungen oder Künstliche Intelligenz (KI), um ihre Taten durchzuführen oder zu verschleiern. Ihre digitalen Kommunikationsformen fordern die

Konto
DKB Bank

IBAN
DE15 1203 0000 0001 2286 59

BIC
BYLADEM1001

Polizeien und erfordern neue polizeiliche Befugnisse und Methoden, um die Bedrohungen gegenüber unseren Bürgerinnen und Bürgern abzuwenden

Damit die sächsische Polizei diesen Entwicklungen entgegenwirken kann, braucht sie ausreichend rechtliche Befugnisse, die auch den Einsatz moderner Technik – wie automatisierte Datenanalyse, dem biometrischen Abgleich von öffentlichen Daten oder den Einsatz von Künstlicher Intelligenz – erlauben.

Ein modernes „Polizeigesetz“ sorgt also dafür, dass die Polizei mit der technischen Entwicklung und den auftretenden Gefährdungslagen Schritt halten kann.

Gleichzeitig schafft dieser aktuelle Gesetzentwurf eine Rechtssicherheit. Er legt genau fest, was die sächsische Polizei in Bezug auf moderne Befugnisse darf und wo deren Grenzen liegen. Das schützt sowohl die Bürgerrechte als auch die Polizistinnen und Polizisten selbst. Wenn die gesetzlichen Regelungen klar und zeitgemäß sind, können Missverständnisse und Rechtsverstöße vermieden werden.

In der Gesamtbetrachtung der Sicherheitsarchitektur der Bundesrepublik Deutschland mit ihren unterschiedlichen Sicherheitsbehörden darf der Freistaat Sachsen in Bezug auf ein modernes, zukunftsfähiges und rechtssicheres Polizeigesetz kein weißer Fleck bleiben. Trotz der Tatsache, dass eine große Anzahl an Befugnissen notwendigerweise fortentwickelt und auch einige neue Befugnisse ergänzt wurden, ist dieser Entwurf keinesfalls ein Vorreiter in der Bundesrepublik. Vielmehr passt sich der Freistaat an die umliegenden Bundesländer an, ohne dass er selbst Innovationspotential entwickelt.

Damit ist Sachsen keinesfalls ein Vorreiter eines neuen und modernen Polizeigesetzes, sondern schließt vielmehr die Lücke zu unseren Nachbarländern. Auch ist dieses Mitziehen in Hinblick auf das Bundesprojekt P20 und dem zentralem Datenhaus mit bundesweit angewandten Applikationen eine zwingende Voraussetzung für ein abgestimmtes und gemeinsames Tätigwerden zur Gefahrenabwehr.

Uns als GdP Sachsen ist bewusst, dass mit der Veränderung oder gar der Ausweitung von Befugnissen immer ein Spagat zwischen den Freiheitsrechten des Einzelnen und dem Sicherheitsbedürfnis der Allgemeinheit geschaffen werden muss.

Ein wichtiger Gradmesser dafür ist das Vertrauen und das subjektive Sicherheitsempfinden der Bevölkerung. Das größte Vertrauen hat die sächsische Bevölkerung im Vergleich mit anderen demokratischen Institutionen in ihre Polizei. Damit steht sie indirekt unterstützend hinter ihren Polizistinnen und Polizisten, weil diese verantwortungsbewusst und vertrauensvoll mit den ihnen zur Verfügung gestellten Befugnissen umgehen.

Nur wenn die Menschen wissen, dass die Polizei wirksam, aber auch fair und rechtsstaatlich handelt, behalten sie ihr Vertrauen in den Freistaat Sachsen und seine Sicherheitsorgane. Ein modernes Sächsisches Polizeivollzugsdienstgesetz trägt dazu bei, weil es Transparenz fördert, einen ausreichenden Rahmen zur Gefahrenabwehr schafft und sicherstellt, dass polizeiliche Maßnahmen verhältnismäßig bleiben.

Die GdP Sachsen begrüßt grundsätzlich den eingereichten Gesetzentwurf!

II. Stellungnahme zu konkret ausgewählten Paragraphen

Artikel 1

Änderung des Sächsischen Polizeivollzugsdienstgesetzes

§ 4

Begriffsbestimmungen

- x. Tiere: Tiere sind keine Sachen. Auf sie sind die für Sachen nach diesem Gesetz vorgeschriebenen Vorschriften entsprechend anzuwenden.
- y. Straftat/Ordnungswidrigkeit:
Eine Straftat im Sinne dieses Gesetzes ist eine rechtswidrige Handlung, die den Tatbestand eines Gesetzes verwirklicht, die mit Strafe bedroht ist.
- Eine Ordnungswidrigkeit im Sinne dieses Gesetzes ist eine rechtswidrige Handlung, die den Tatbestand eines Gesetzes verwirklicht, die die Ahndung mit einer Geldbuße zulässt.

Die Neudefinition einzelner Begriffe kann befürwortet werden. Es wird angeregt, zusätzliche Nummerierungen für die grundsätzliche Einordnung zu Maßnahmen von „Tieren“ sowie zur Begriffsbestimmung von „Straftaten und Ordnungswidrigkeiten“ einzufügen.

Dabei sollen im Bezug auf Tiere die unterschiedlichen Regelungen im Gesetz ersetzt werden bzw. zur Rechtsklarheit beitragen

§ 12a

Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme

Positiv zu bewerten ist, dass die Drohnenabwehr als Aufgabe ins Polizeivollzugsdienstgesetzes aufgenommen wurde, um auf die weiter ansteigende Gefährdungslage zu reagieren.

Ungeachtet der Schaffung dieser notwendigen rechtlichen Befugnis muss eine Abstimmung mit allen wesentlichen Partnern zu Drohnenabwehr deutlich intensiviert werden. Der Schutz der Bevölkerung kann isoliert von jeder Behörde (Bundeswehr, Bundespolizei oder Landespolizei) betrachtet werden.

Allein schon aufgrund der unterschiedlichen Verantwortungsbereiche mit den dazugehörigen Befugnissen (stark vereinfacht: Bundeswehr Angriffsgefährdung von außerhalb Deutschlands, Bundespolizei Angriffsgefährdung auf bestimmten Gebieten innerhalb Deutschlands und die Landespolizei zur Angriffsgefährdung des restlichen Gebietes des Freistaates) muss zukünftig ein „Verteidigungskonzept“ auf Bundesebene erarbeitet werden.

Die o. g. Behörden haben unterschiedliche Philosophien bei der Beseitigung dieser Gefährdungslage. Während der Bundeswehr eine Vielzahl von technischen Mitteln bis hin zum Abschuss mittels Kriegsgerät zur Verfügung steht, verfolgen die Bundespolizei wie auch die Landespolizei mit Blick auf die Urbanisierung der Fläche einen anderen Ansatz. Hier kommt ohne

Frage nur die Übernahme der Steuerungsfähigkeit der Drohnen (Laser, Jammer etc.) und das gesicherte zu Boden bringen (notfalls mittels „Fangnetz“ mit Fallschirm) in Frage. Nur so kann die Bevölkerung von einer unkontrolliert herabstürzenden Drohne bewahrt werden.

§ 15

Identitätsfeststellung, Prüfung von Berechtigungsscheinen

Abs. 1

Nr. 5

wenn sie sich in einem Fahrzeug befindet, das zur gezielten Kontrolle **nach § 60 Abs. 1** ausgeschrieben ist und tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme zur Abwehr einer Gefahr erforderlich ist;

Nr. 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, Nummer 4 oder Absatz 2 Nummer 4 des Sächsischen Versammlungsgesetzes oder gemäß § 31a des Sächsischen Polizeibehördengesetzes zu verhindern;

Die Einfügung von „**nach § 60 Abs. 1**“ in Nr. 5 dient der Klarstellung bzw. Vereinfachung in der Rechtsanwendung.

Die Einfügung von „**oder Straftaten**“ in Nr. 6 dient der Klarstellung in der Rechtsanwendung. Es kann vom Verfasser sicher nicht gewollt sein, dass Identitätsfeststellungen zur Straftatenverhinderung lediglich in Kontrollstellen in Verbindung mit dem Versammlungsgesetz getätigt werden dürfen, nicht jedoch für weitere Gesetze. In der Begründung zum Entwurf wurde von einer Überführung und Konkretisierung des alten Regelungsgehalts gesprochen.

§ 19

Maßnahmen zum Schutz vor häuslicher Gewalt und sonstigen Nachstellungen

Die Konkretisierung und Erweiterung der Gefahrensituation vor allem im Zusammenhang mit häuslicher Gewalt erleichtern deutlich den polizeilichen Alltag. Die daraus resultierenden Gebote bzw. Verbote sind eine notwendige Anpassung an die Lebenssachverhalte und Anwendungsfälle zum Schutz betroffener Personen.

Abs. 1

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

1. die Person, von der die Gefahr ausgeht, aus einer gemeinsam mit der gefährdeten Person genutzten Wohnung und dem unmittelbar angrenzenden Bereich verweisen und ihr die Rückkehr dorthin untersagen, sowie
2. der Person, von der die Gefahr ausgeht, verbieten,
 - a) sich in einem bestimmten Umkreis der Wohnung der betroffenen Person aufzuhalten,
 - b) Orte zu betreten, an denen sich die gefährdete Person oder bestimmte ihr nahe stehende Personen regelmäßig aufhalten werden,
 - c) Verbindung zur gefährdeten Person auch unter Verwendung von Fernkommunikationsmitteln aufzunehmen **und oder**
 - d) ein Zusammentreffen mit der gefährdeten Person herbeizuführen.

Die Anordnungen sind zu befristen; die Frist kann verlängert werden.

Maßnahmen nach Satz 1 enden **spätestens** mit dem Ablauf des 14. Tages nach ihrer Anordnung, soweit nicht die Polizei im Einzelfall eine kürzere Frist festlegt.

Stellt die gefährdete Person während der nach Satz 3 bestimmten Dauer der Maßnahmen einen Antrag nach dem Gewaltschutzgesetz, enden die Maßnahmen mit dem Tag der gerichtlichen Entscheidung oder des gerichtlichen Vergleichs, **spätestens jedoch mit Ablauf des 14. Kalendertages nach dem Ende der nach Satz 3 bestimmten Dauer.**

Die Anordnungen nach Satz 2 sind sofort vollziehbar.

Die in Abs. 1 Nr. 2 benannten Personen sind als mögliche Varianten einer Gefahrensituation zu sehen. Insofern müsste an Ende der Variante c ein „**oder**“ statt einem „**und**“ stehen.

Eine Anordnung ist zu befristen und sollte eine Frist unterhalb der maximal erlaubten Dauer beinhalten, welche auch verlängert werden kann. Die Ergänzung durch „**spätestens**“ stellt klar, dass die in Satz 2 betroffene (Gesamt)Frist jedoch maximal bis zum Ablauf des 14. Tages ab der Anordnung des Verwaltungsaktes zulässig ist.

Die Ergänzung zur sofortigen Vollziehbarkeit macht deutlich, dass der Einspruch gegen diese Anordnung keine aufschiebende Wirkung hat und die polizeiliche Maßnahme sofort vollzogen werden kann. Dies dient der besseren Durchsetzbarkeit, da diese Anordnungen meist in Eilfällen erfolgen müssen.

Irreführend hingegen ist die vorgeschlagene Regelung im Satz 4 Halbsatz 2. Meint der Verfasser damit, dass die vom Schutz betroffene Person einerseits 14 Tage Schutz durch die Anordnung der Polizei genießt und ggf. am letzten Tag dieser Frist bei Gericht einen Antrag auf eine gerichtliche Entscheidung einreicht und dadurch weitere 14 Tage Schutz genießt?

Sollte sich die GdP Sachsen bei der o. g. Annahme irren, muss angemerkt sein, dass aufgrund des vorgeschriebenen Verfahrensweg:

1. Einsatzmaßnahme Polizei mit Dokumentation und Belehrung
2. Kontaktaufnahme durch Hilfseinrichtung/ Schutzeinrichtung möglichst am Folgetag mit Terminfindung Beratungsgespräch (ggf. Hinzuziehung Dolmetscher notwendig)
3. Beratungsgespräch in der Hilfseinrichtung z.B. DIG – Dresdner Interventions- und Koordinierungsstelle zur Vorbereitung eines Antrages bei Gericht
4. Ggf. Kontaktaufnahme mit Rechtsanwalt mit Terminfindung zur Erstellung Antrag bei Gericht (ggf. Hinzuziehung Dolmetscher notwendig)
5. Gespräch Rechtsanwalt
6. Antrag bei Gericht
7. Entscheidung durch Gericht meist mit Rücksprache und Aktenvorlage durch die Polizei,

die Anordnungsfrist bis zur der familiengerichtlichen Entscheidung zu eng bemessen ist. Auch werden zur Risikoeinschätzung der Gesamtsituation regelmäßige mehrmalige Vernehmungen bei der Polizei durchgeführt. Aus dieser ergeben sich zusätzlich ggf. weitere Maßnahmen / Verwaltungsakte z.B. § 21 Aufenthalts- und Kontaktverbot, § 22 Gewahrsam oder § 61 elektronische Aufenthaltsüberwachung.

Auch ist für die Verlängerung der Anordnungsfrist bis zur gerichtlichen Entscheidung die Polizei nach diesem Gesetz verantwortlich, was wiederum Auswirkung auf die Belastung des angespannten Personalkörpers hat.

§ 21

Aufenthaltsanordnung und Kontaktverbot

Positiv ist die Novellierung in Bezug auf die Abgrenzung zwischen Aufenthaltsgebot und -verbot und den Wegfall der zeitlichen Begrenzung des Verwaltungsaktes zu bewerten. Damit wurde die Anwendbarkeit und damit die rechtliche Entwicklung an Lebenssachverhalte angepasst und dient der Verwaltungsvereinfachung und Belastungsminimierung für die sächsische Polizei.

§ 28

Durchsuchung von Sachsen

Nr. 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 **nach § 60 Abs. 1** ausgeschrieben ist; die Durchsuchung kann sich auch auf die in diesem Fahrzeug enthaltenen oder mit dem Fahrzeug verbundenen Sachen erstrecken,

Nr. 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

Nr. 8

es sich um ein Fahrzeug handelt, das zur gezielten Kontrolle **nach § 60 Abs. 1** ausgeschrieben ist und tatsächliche Anhaltspunkte dafür vorliegen, dass die Durchsuchung zur Abwehr einer Gefahr erforderlich ist“.

Die Einfügung von „**nach § 60 Abs. 1**“ in Nr. 5 und 7 dient der Klarstellung bzw. Vereinfachung in der Rechtsanwendung.

§ 29

Betretung und Durchsuchung von Wohnungen

Die Übernahme der Nachtzeitschranken aus der StPO dient zur Verwaltungsvereinfachung und ist zu begrüßen.

§ 40

Begriff und Mittel des unmittelbaren Zwangs

Als GdP Sachsen begrüßen wir ausdrücklich die Streichung „von Spezialeinheiten“ im Abs. 4 Satz 2 und die damit verbundene Möglichkeit, für die sächsische Polizei das Distanz-Elektro-Impuls-Gerät (DEIG) als Mittel des unmittelbaren Zwangs zum Einsatz zu bringen.

Dabei ist für die GdP Sachsen durchaus vertretbar, dass es sich beim DEIG um ein Waffe im Sinne des SächsPVDG handelt, da ähnlich einer Schusswaffe mittels eines Abzugs ausgelöst zwei Pfeile mittels Stickstoffgas abgeschossen werden. Vertretbar wäre aber auch bei einem minderschweren Einsatz - lediglich als „Elektroschocker“ - die Einordnung als Hilfsmittel der einfachen körperlichen Gewalt.

Für die GdP Sachsen steht fest: Das DEIG hat sich in der Praxis vieler Polizeien sowohl im Bundesgebiet als auch europa- /weltweit bewährt. Studien zeigen, dass die bloße Androhung der Anwendung des DEIG beim polizeilichen Gegenüber auch in Befürchtung der möglichen Wirkung auf dessen Körper zu einer deutlich positiveren Reaktion führte als die schwerwiegendere Androhung und Wirkung des Einsatzes einer Schusswaffe.

Auch darf man nicht verkennen, dass das DEIG die gefährliche Lücke bei der Verzögerung im Sinne der Wirksamkeit anderer polizeilicher Hilfsmittel (z. B. Reizstoffsprüngerät) bis hin zur Schusswaffe in der Nahdistanz schließt. Alle bis dato zulässigen Mittel des unmittelbaren Zwangs setzen nach dem Einsatz deutlich verzögert ein, wodurch es dem „Angreifer“ möglich ist, seinen Angriff weiter fortzusetzen und die Distanz bis zum Opfer ggf. weiter zu verkürzen.

Anders ist die Wirkung beim DEIG. Nach dem Abschuss der ca. 2,5 cm kurzen Pfeile leiten diese nach dem Auftreffen mittels dünner Drähte einen Strom (mit niedriger Ohmzahl) in den Körper des Ziels. Die Stromimpulse sind so gewählt, dass diese zu einer sofortigen Verkrampfung der zwischen den Elektroden liegenden Muskeln führen. Die Verkrampfung der Muskulatur erfolgt unabhängig von einem z. B. durch Drogen oder Alkohol herabgesetztem Schmerzempfinden. Dadurch kann das polizeiliche Gegenüber seine gefährdenden Handlungen nicht fortsetzen.

Der Strom wird nach kurzer Zeit automatisch unterbrochen, danach ist die getroffene Person sofort wieder ansprechbar, aber je nach Situation und Konstitution nicht sofort wieder vollständig handlungsfähig. Durch diese Wirkung ist es möglich, gefährliche Situationen frühzeitig zu entschärfen, bevor es zu schwerwiegenden Verletzungen oder gar zum Schusswaffengebrauch kommt.

Auch können mögliche Einsätze des DEIG bei Personen mit suizidaler Absicht aufgrund der voran geschilderten Einflussnahme und der Wirksamkeit positive Erfolge im Sinne der Verhinderung unterstellt werden.

Der gesetzte Zeitraum für die Erfahrungsermittlung wird durch die GdP Sachsen grundsätzlich mitgetragen, da mit Blick auf die engen Haushaltsmittel eine Beschaffung als Mann-Ausstattung und als flächendeckender Einsatz im Streifendienst und den geschlossenen Einheiten nicht realisierbar ist.

Aus diesem Grund regt die GdP Sachsen für den Erprobungszeitraum auch ein angepasste Ausstattung analog der Mehrzweckpistole (MZP) in den geschlossenen Einheiten an. Dass kann bedeuten, dass z.B. nur einzelne und geeignete Kolleginnen und Kollegen einer Dienstgruppe in einem Polizeirevier mit einer Ausstattung des DEIG bedacht werden. Sollte es zu einem möglichen Einsatzfall kommen, werden ggf. die ausgerüsteten Kolleginnen und Kollegen zum Einsatzort verlegt.

Auch bedarf es in Vorbereitung der Einführung eines umfassenden Aus- und Weiterbildungskonzeptes für die betreffenden Kolleginnen und Kollegen mit entsprechenden Trainings. Die möglichen Risikofaktoren können dabei aufgegriffen werden.

Damit ist klar: Es gibt keine sachlichen Gründe, von der grundsätzlichen Einführung des DEIG in der sächsischen Polizei abzugehen. Es ein unverzichtbarer Baustein moderner, vielseitiger und verhältnismäßiger Polizeiarbeit

Das DEIG ist ein hocheffizientes und lebensrettendes Einsatzmittel, das in den meisten Fällen bereits durch die bloße Androhung Konfliktsituationen entschärft.

§ 57**Offener Einsatz technischer Mittel zur Bild- und Tonaufnahme und -aufzeichnung**

Die GdP begrüßt die Novellierung dieses Paragraphen, denn damit wird die durch höchst-richterliche Entscheidung notwendige Klarstellung und Anpassung vorgenommen.

Abs. 4ff

Auch wenn die Konstellation des Einsatzes im Kernbereich der privaten Lebensgestaltung in Bezug auf Maßnahmen z. B. in Zusammenhang mit häuslicher Gewalt beschrieben ist, stellt dieses nach wie vor eine schwierige Einsatzkonstellation dar.

Abs. 4:

Die Polizei kann bei der Durchführung von Maßnahmen zur Gefahrenabwehr **oder zur Verfolgung von Straftaten oder Ordnungswidrigkeiten** durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen personenbezogene Daten kurzzeitig in einem Zwischenspeicher für 60 Sekunden erfassen (**Pre-Recording**), soweit und solange dies mit hinreichender Wahrscheinlichkeit zum Schutz der eigenen oder einer dritten Person gegen eine Gefahr für Leib oder Leben erforderlich ist.

In Wohnungen ist eine Maßnahme nach Satz 1 nur zulässig, wenn dies mit hinreichender Wahrscheinlichkeit zur Abwehr einer dringenden Gefahr für Leib oder Leben der eigenen oder einer dritten Person **oder eine Gefahr für Sachen von bedeutendem Wert** erforderlich ist.

Satz 2 gilt nicht für Arbeits-, Betriebs- oder Geschäftsräume während der Öffnungszeiten und wenn die Maßnahme während der Öffnungszeiten durchgeführt wird

Die erlangten Daten sind automatisiert nach höchstens 60 Sekunden zu löschen, soweit die Voraussetzungen für eine Aufzeichnung nach Abs. 5 nicht vorliegen.

Durch die Ergänzung „**oder zur Verfolgung von Straftaten oder Ordnungswidrigkeiten**“ im Abs. 4 Satz 1 wird zugestanden, dass eine Gefahrenlage nicht nur bei Maßnahmen der Gefahrenabwehr, sondern auch im Rahmen der Verfolgung von Straftaten und Ordnungswidrigkeiten besteht. Deshalb kann auch in derartigen Fälle die Maßnahme angewendet werden.

Durch die Ergänzung „(**Pre-Recording**)“ im Abs. 4 Satz 1 wird deutlich gemacht, dass es sich bei der Aufnahme um eine durch das Gerät retrograde Aufzeichnung vor der manuellen Speicherung nach Abs. 5 handelt.

Durch die Ergänzung „**oder eine Gefahr für Sachen von bedeutendem Wert**“ im Abs. 4 Satz 2 wird zugestanden, dass im täglichen Dienst Einsätze bewältigt werden, in dem häufig eine Gefahr für Sachen besteht, ohne dass Personen gefährdet werden.

Der GdP Sachsen erschließt sich nicht, was durch den Verfasser mit Satz 3 des Abs. 4 genau ausgesagt werden soll.

Handelt es sich um eine weitere Konkretisierung und besonderer Anwendungsfall des Satzes 1, welcher jedoch keine besonderen Schranken oder Maßnahmen nach sich zieht? Alternativ könnten damit auch Arbeits-, Betriebs- oder Geschäftsräume innerhalb einer Wohnung gemeint sein, was jedoch aus dem Entwurf mit Begründung nicht deutlich genug heraus gestellt ist. Dabei scheint auch eine notwendige redaktionelle Anpassung des Satz aufgrund der doppelten Nennung „während der Öffnungszeiten“ notwendig.

Des Weiteren wird aufgrund des Zusammenhangs vorgeschlagen, dass der letzte Satz des Abs. 5 an das Ende des Abs. 4 verschoben wird.

Abs. 5:

Die Speicherung (Aufzeichnung) der erlangten Daten über 60 Sekunden hinaus ist:

- a) nach Absatz 4 Satz 1 nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz der eigenen oder einer dritten Person gegen eine Gefahr für Leib oder Leben oder für Sachen von bedeutendem Wert erforderlich ist.
- b) nach Absatz 4 Satz 2 nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz der eigenen oder einer dritten Person gegen eine dringende Gefahr für Leib oder Leben oder für Sachen von bedeutendem Wert erforderlich ist.

~~Die erlangten Daten sind automatisiert nach höchstens 60 Sekunden zu löschen, soweit die Voraussetzungen für eine Aufzeichnung nicht vorliegen.~~

Durch die Neuordnung wird eine bessere Übersichtlichkeit erzeugt. In den Alternativen a) und b) wird die Ergänzung „*oder für Sachen von bedeutendem Wert*“ mit gleicher Begründung wie in Abs. 4 vorgeschlagen.

Abs. 6:

In Bereichen, die der Ausübung von Tätigkeiten von Berufsheimnisträgern nach den §§ 53 und 53a der Strafprozessordnung dienen, sind Maßnahmen nach Absatz 4 und 5 unzulässig.

Ergeben sich während der Durchführung einer Maßnahme nach Absatz 5 Satz 2 tatsächliche Anhaltspunkte dafür, dass der Kernbereich privater Lebensgestaltung betroffen ist, ist die ~~Maßnahme Aufnahme~~ unverzüglich zu unterbrechen.

Die ~~Maßnahme Aufnahme~~ darf fortgeführt werden, wenn keine Anhaltspunkte mehr dafür vorliegen, dass der Kernbereich privater Lebensgestaltung betroffen ist.

Soweit ~~Erkenntnisse Aufnahmen~~ aus dem Kernbereich privater Lebensgestaltung durch eine Maßnahme nach Satz 2 ~~erlangt gefertigt~~ 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.

Zur Klarstellung wird angeregt, dass die in den Sätzen 2 und 3 benannten „Maßnahmen“ klarstellend in „Aufnahme“ geändert werden.

Ebenso wird angeregt, in Satz 2 das Wort „unverzüglich“ anzufügen. Unstrittig ist, dass Aufnahmen im Kernbereich der privaten Lebensgestaltung auf ein Mindestmaß beschränkt bzw. untersagt sind. Denn das grundsätzliche Einschreiten von Polizeibeamten z. B. bei gegenwärtigen Körperverletzungen sollte nicht unterbrochen werden, nur weil der Täter ins Schlafzimmer flüchtet und die Polizeibeamtinnen und Polizeibeamten erst die Aufzeichnung beenden müssen.

Zur Klarstellung wird angeregt, dass die in Satz 3 benannten „Erkenntnisse“ klarstellend in „Aufnahme“ geändert werden.

Aufgrund des unmittelbaren Zusammenhangs zu den Maßnahmen nach den Absätzen 2 und 3 wird angeregt, dass der Abs. 12 direkt nach dem Abs. 3 verortet werden sollte.

Abs. 8:

Die Aufzeichnungen nach den Absätzen 4 und 5 durch körpernah getragene Geräte sind verschlüsselt sowie manipulationsgesichert zu fertigen und aufzubewahren.

Die angefertigten Bild- und Tonaufnahmen sind nach Ablauf von ~~einem Monat~~ 30 Tagen zu löschen sowie daraus gefertigte Unterlagen zu vernichten, soweit sie nicht für Zwecke der Strafverfolgung, zur Verfolgung von Ordnungswidrigkeiten oder für die Überprüfung der Rechtmäßigkeit einer aufgezeichneten Maßnahme oder der Aufzeichnung benötigt werden.

Auf Antrag erhalten betroffene Personen Einsicht in die Aufzeichnung. Die betroffenen Personen sind über das Bestehen des Rechts auf Einsichtnahme zu informieren.

Näheres zum Verfahren regelt das Staatsministerium des Innern durch Verwaltungsvorschrift. *Die weitere Verarbeitung der nach Absatz 5 Satz 2 erlangten Daten ist nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt wurde.*

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

Es wird angeregt, dass die Wörter „einem Monat“ im Satz 2 durch die Formulierung „30 Tagen“ ersetzt werden. Die vorgeschlagene Formulierung lässt sich besser nachvollziehen bzw. technisch (automatisiert) umsetzen.

Es wird vorgeschlagen, dass im Satz 2 die Formulierung „zur Verfolgung von Ordnungswidrigkeiten“ ergänzt wird, da nicht nachvollzogen werden kann, dass in allen anderen Anwendungsfällen des § 57 Bild- und Tonaufnahmen zur deren Verfolgung herangezogen werden können, bei den Anwendungsfällen des Abs. 3 und 4 ausdrücklich nicht.

Durch die GdP Sachsen kann rechtlich nicht abschließend bewertet werden, ob die Adressierung in Satz 4 zu richterlichen Entscheidung zutreffend ist. Für die Verwendung der Bild- und Tonaufnahmen in Strafsachen ist die Staatsanwaltschaft zuständig. Dies müsste auch jene Bild- und Tonaufnahmen in Wohnungen betreffen.

Abs. 9:

Die Polizei darf im öffentlichen Verkehrsraum personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Bildübertragung und -aufzeichnung zur Verhütung von Verstößen gegen die **Verkehrsvorschriften der § 4 Abs.3, § 8, § 9, des § 23 Absatz 1a sowie § 37 Abs. 2 Nr. 1** Straßenverkehrs-Ordnung erheben, sofern tatsächliche Anhaltspunkte bestehen, dass an bestimmten Streckenabschnitten oder Verkehrsknotenpunkten in regelmäßiger Weise gegen die genannte Vorschrift verstoßen wird oder es sich in sonstiger Weise um einen Bereich mit besonderer Unfallträchtigkeit handelt.

Die Bildaufzeichnungen dürfen das Fahrzeug, das Kraftfahrzeugkennzeichen sowie Informationen über Ort, Zeit, Fahrtrichtung und die fahrzeugführende Person erfassen.

Ergibt sich kein Hinweis auf einen Verkehrsverstoß, sind die Bilddaten unverzüglich, spätestens jedoch mit der Beendigung der Maßnahme zu löschen.

Aufgezeichnete Daten, die nicht unverzüglich zu löschen sind, dürfen ausschließlich zum Zweck der Verfolgung und Ahndung von Verstößen gegen die in Satz 1 bezeichneten Verkehrsvorschriften verarbeitet werden.

Positiv zu bewerten ist auch die Schaffung der Möglichkeit der offenen Bildübertragung und -aufzeichnung im öffentlichen Verkehrsraum zur Verhinderung von Verkehrsordnungswidrigkeiten. Die bedeutende Aufgabe der Verkehrs-Sicherheitsprävention und -überwachung und damit verbundener Reduzierung von Gefährdungslagen kann nur durch den aktiven Dienst und Kontrolltätigkeiten erfüllt werden. Dazu gehört auch der Einsatz neuer und personalentlastender technischer Mittel. Nur durch entsprechenden Kontrolldruck und mit Einsatz zeitgemäßer Technik kann der gewünschte Erfolg bei der Reduzierung der Unfallzahlen aufgrund verschiedenster Unfallursachen erzielt werden.

Bedauerlicherweise wird in der Novellierung lediglich auf die Überwachung des § 23 Abs. 1a StVO abgestellt, da die Nutzung von Kommunikationsmitteln eine bedeutende Unfallursache darstellt.

Jedoch ergeben sich gleichgelagert weitere Gefährdungslagen, die überwacht werden sollten, wie z. B. Ordnungswidrigkeiten im Bereich der Rotlicht-, Abstands-, Geschwindigkeits- und Vorfahrtverstöße.

Es wird angeregt, dass der Anwendungsbereich auf Verkehrsvorschriften der § 4 Abs.3 (konkreter Abstand von LKW), § 8 (Vorfahrtregeln), § 9 (Abbiegen, Wenden und Rückwärtsfahren), § 23 Absatz 1a (elektronische Geräte der Kommunikation) sowie § 37 Abs. 2 Nr. 1 (Wechsellichtzeichen) in der Straßenverkehrsordnung erweitert wird.

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

Die GdP Sachsen begrüßt ausdrücklich die Einführung, da dieser Paragraph die Lücke schließt, die aufgrund begrenzter personeller Ressourcen und in meist kurzen Reaktionszeiträumen nicht vollumfänglich geleistet werden kann. Mit dieser neuen Maßnahme bekommt die sächsische Polizei eine ermittlungstechnische Unterstützung durch die Möglichkeiten spezielle Bewegungsmuster von Person oder Waffen bzw. gefährliche Gegenstände auf polizeilichen Übersichtsaufnahmen automatisch zu identifizieren und zu verfolgen. Die Echtzeitanwendung ermöglicht es der Polizei noch während der Maßnahme vor Ort eine Überprüfung der Erkenntnis durchzuführen.

Die Gefahrensituationen wurden spezifisch für den Einsatz geregelt und für die Echtzeitanwendung gesondert verschärft, um eine Überbeanspruchung dieser Rechtsnorm zu vermeiden. Dennoch besteht die Gefahr, dass die automatisierte Verarbeitung die komplexen Besonderheiten bei Bild- und Tonaufnahmen oder -aufzeichnungen von Personen nicht im perfekten Maße umsetzt.

Einer daraus resultierende Fehleranfälligkeit kann stets durch eine manuelle Prüfung des Ergebnisses und ggf. Nachjustierung der Verarbeitung (z.B. Neusetzen des zu markierenden Gegenstands) analog zu §62b Absatz 2 entgegengewirkt werden.

Leider ist die Maßnahme aufgrund der Zuschreibung auf § 57 Abs. 2 und 3 nicht auf weiteres Datenmaterial ausgelegt, das nicht offen bzw. nicht durch den PVD erhoben wurde (gespeicherte Aufnahmen von Privatpersonen/Unternehmen, Videoüberwachung durch Kommunen, TV-Übertragungen, Webcams oder Livestreams). Hier besteht aus polizeifachlicher Sicht Regelungsbedarf.

Selbstredend kann diese Maßnahme bei Aufnahmen von Dritten nicht in Echtzeit durchgeführt werden, aber eine nachträgliche Identifikation kann hilfreich sein. Leider fehlt im Entwurf der Hinweis, was unter Echtzeit verstanden wird – also wie groß der zeitliche Abstand sein muss, damit die weniger eingreifende Norm aus Absatz 1 greift.

Im §57 ist eine Überschreitung der Daten nach 60 Sekunden vorgeschrieben, im Sinne einer einheitlichen Bewertung wird diese Zeitspanne für die Echtzeitdefinition seitens der GdP befürwortet.

In einer Echtzeit-Anwendung müssen Daten aus der Bild- und Tonaufnahmen auch durch den Einsatz von ermittlungstechnischer Unterstützung zum Auffinden von Gefährdern oder Stören oder zum Auffinden von Opfern oder vermissten Personen genutzt werden dürfen.

Für die GdP Sachsen besteht grundsätzlich kein veränderter Grundrechtseingriff, wenn die Polizei selbst manuell und mit vielen Beamten die Aufzeichnungen auswerten darf, aber eine besondere Schwelle beim Einsatz ermittlungsunterstützender Software geschaffen wird.

§ 58**Anlassbezogene automatisierte Kennzeichenerkennung**

Positiv wird durch die GdP Sachsen die klarstellende Anwendung zur Umsetzung der höchst-richterlichen Entscheidungen bewertet. Damit verbunden ist auch die Ausweitung der Anwendungsbereiche und die Anpassung auf Lebenssachverhalte von Fahndungsgründen im polizeilichen Alltag, auch wenn z. B. eine Parallelkompetenz im § 163g StPO existiert.

Grundsätzlich kann gesagt werden, dass diese automatisierte Datenabfrage ggf. gleichzeitig in den unterschiedlichsten polizeilichen Fahndungslisten von Kennzeichen das polizeiliche Handeln deutlich unterstützt und die durch fehlendes Personal entstandene Belastung durch reduziert.

§ 60**Ausschreibung von Personen und Sachen**

Die GdP Sachsen befürwortet die Neustrukturierung des Paragraphen zur Ausschreibung von Personen und Sachen. Jedoch muss kritisch angemerkt werden, dass die Streichung der Möglichkeit zur Ausschreibung von Kontakt- und Begleitpersonen ggf. eine erhebliche Reduzierung des Fahndungserfolges von Gefährdern nach sich ziehen kann.

Potentiale Störer oder Gefährder in bestimmten Deliktsbereichen (z. B. mit terroristischen Hintergrund) versuchen, sich verdeckt im Landesinneren zu bewegen oder über Mittelsmänner zu kommunizieren. Meist läuft dies mit Unterstützung über ihnen nahestehende Personen. Ein wichtiger Ansatzpunkt für einen Fahndungserfolg ist weiterhin die Möglichkeit der Ausschreibung von Kontakt- und Begleitpersonen, welche regelmäßig weniger verdeckte Aktionen durchführen.

Darüber hinaus müssen in Abs. 2 alle der in Abs. 1 ausgeschriebenen Varianten aufgeführt sein, da sonst die Ausschreibung und Rückmeldung nicht in Einklang sind. Es wird davon ausgegangen, dass die Nennung „Containers“ versehentlich vergessen wurde.

§ 61**Elektronische Aufenthaltsüberwachung**

Die GdP Sachsen begrüßt die Novellierung dieses Paragraphen, weil sie die polizeilichen Lebenssachverhalte aufgreift und positive Klarstellung der Anwendungsbereiche ausweist.

Grundsätzlich kann gesagt werden, dass diese Elektronische Aufenthaltsüberwachung das polizeiliche Handeln deutlich unterstützt und die Belastung durch fehlendes Personal reduziert. Positiv kann sich dies beim Einsatz zur Unterbindung häuslicher Gewalt und Verhinderung von Femiziden auswirken.

Für die Risikoeinschätzung der Gesamtsituation (z.B. mittels Odara-Bogen), welche zur Beurteilung und Beantragung die Grundlage darstellt, sind regelmäßig mehrmalige

Vernehmungen der (Opfer)Zeugen oder Beschuldigten bei der Polizei durchzuführen. Damit einhergehend verlängert die Polizei auch Anordnungsfrist einer Maßnahme nach §19 bis zur gerichtlichen Entscheidung die Polizei.

Es wird angeregt, dass in Rahmen der nach Abs. 7 festgelegten Erfahrungszeitraums ein moderne Variante der elektronischen Aufenthaltsüberwachung nach dem Züricher- bzw. spanischem Modell im Zusammenhang mit Maßnahmen nach § 19 erprobt werden. Dieses sollte in Zusammenhand mit der Justiz erfolgen.

§ 62a

Anlassbezogene Anwendung zur automatisierten Datenanalyse

Die GdP Sachsen begrüßt, dass durch eine einfachere, schnellere und wirksamere Auswertung der bereits vorhandenen polizeilichen Informationen die Auswertung sehr großer und komplexer Datenmengen möglich gemacht werden soll. Diese Ermittlungsunterstützung beim Zusammenführen (Data Mining) von vorhandenen Massendaten in den (polizeilichen) Datenbanken ist aus polizeifachlicher Sicht zwingend erforderlich, da die Dimensionen und die Vielseitigkeit dieser Daten das menschliche Wirken übersteigen.

Durch die Einführung dieses Paragraphen wird Gefahren-Lücke in der Auswertung geschlossen, die aufgrund begrenzter personeller Ressourcen nicht vollumfänglich geleistet werden kann.

Mit dieser neuen Maßnahme bekommt die sächsische Polizei eine ermittlungstechnische Unterstützung durch die Verknüpfung von Erkenntnissen aus verschiedenen Datenbeständen. Die Notwendigkeit und der Mehrwert dieser Rechtsnorm und der damit möglichen Maßnahmen zeigt sich bereits in den Erprobungen anderer Bundesländer.

Die GdP begrüßt die Berücksichtigung bisheriger Gerichtsurteile im hiesigen Entwurf durch die Einschränkungen auf Gefahrensituationen für bedeutende Rechtsgüter, ein differenziertes Rollenkonzept, eine Begrenzung der verarbeitbaren Datenbestände und die weiteren in der Rechtsnorm aufgeführten Klarstellungen.

Aktuell besitzt die sächsische Polizei bereits die Befugnisse die zahlreichen Datenbestände abzufragen und zu verarbeiten. Jedoch ist es aufgrund des zusammengetragenen Datenumfangs häufig mit erheblichem Aufwand verbunden, diese Daten korrekt und zeitnah einzuordnen. Eine vorgelagerte automatische Datenanalyse erlaubt eine deutlich schnellere Beurteilung der Lage und erhöht damit die Reaktionsfähigkeit der Polizei und somit des Staates in Gefahrensituationen für bedeutende Rechtsgüter.

Das Verbot von Verkehrsdaten Absatz 3 Nummer 4 stößt seitens der GdP auf Unverständnis. Ohne Frage erhalten erhobene Verkehrsdaten von Sendeanlage in zu hohem Maße die Daten von Unbeteiligten. Dementgegen steht jedoch die Erhebung von Verkehrsdaten einzelner sachrelevanter Geräte (z.B. Fahrzeug oder Mobiltelefon), wo kaum bis keine Daten von Unbeteiligten zu erwarten sind. Nicht zuletzt scheint dieses absolute Verbot auch zu vermeiden, dass Verkehrsdaten in die Analyse einfließen, welche um die Daten der Unbeteiligten bereinigt wurden.

Der für die automatisierte Datenanalyse mögliche Einsatz von Künstliche Intelligenz wird durch die GdP befürwortet. Jedoch sollte zuvor eine intensive Prüfung hinsichtlich möglicher Benachteiligungen durchgeführt werden. Außerdem sollte sichergestellt werden, dass die Künstliche Intelligenz durch deren Anwendung nicht weiterlernt. Die Anwendung ist gegen die jeweiligen Betroffenen ausgelegt, sodass keine entlastende Anwendung für den Betroffenen in Frage kommt und somit einer Verschiebung der Künstlichen Intelligenz nicht entgegenwirken kann.

Die restriktive Auslegung der Internetanbindung wird in Anbetracht der aktuellen Diskussionen über Erprobungen anderer Bundesländer akzeptiert. Die GdP Sachsen befürwortet eine erneute Betrachtung dieses Einsatzes (ggf. als separates System getrennt von den polizeilichen Datenbeständen), nach einer Evaluierung über den Einsatz dieser Rechtsnorm.

Es wird erwartet, dass die sächsische Polizei entgegen der Verfahrensweise eines anderen Bundeslandes erst nach der Einführung dieser Rechtsnorm die Einführung der automatisierten Datenanalyse umsetzt.

Bei der Umsetzung sollte die digitale Souveränität berücksichtigt werden, da der Zugriff auf sehr umfangreiche und sensible Daten ermöglicht wird. Es sollte aktuell ergebnisoffen geprüft werden, ob neben der aktuell eingesetzten, strittigen Lösung anderer Bundesländer die Anwendungen von Rola Security GmbH mit Chapsvision[1], One Data GmbH, Innosystec GmbH, FSZ GmbH, Almato AG[2]. Nicht zuletzt ist zu berücksichtigen, dass es einige Behörden gibt, die ihre bisherigen Beschaffungen wieder verwerfen bzw. die Verträge auslaufen lassen.

Auch mit Blick auf das Projekt P20 und der bundeseinheitlichen IT-Lösung sollte Sachsen die notwendigen Freigabe der Norm erteilen.

[1] <https://www.rola.com/de/insights/rola-und-chapsvision-schliessen-strategische-partnerschaft-fuer-europaeische-big-data-analyseplattform>

[2] <https://www.br.de/nachrichten/deutschland-welt/polizeisoftware-von-palantir-werden-alternativen-ignoriert,UzmaB7J>

Im Abs. 4 Satz 2 der Norm wird von einem Konzept gesprochen, jedoch fordert Satz 1 eine veröffentlichte Verwaltungsvorschrift.

Durch die Einführung dieser allumfassenden neuen Norm muss geprüft werden, dass bereits jetzt im Einsatz befindliche niederschweligen Assistenzsysteme der polizeilichen Ermittlungsarbeit nicht durch diese betroffen sind.

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

Die GdP Sachsen begrüßt ausdrücklich die Einführung, da dieser Paragraph die Lücke schließt, die aufgrund begrenzter personeller Ressourcen nicht vollumfänglich geleistet werden kann. Die Praxis hat gezeigt, dass der Abgleich von gespeicherten biometrischen Daten von Gesichtern mit dem Internet dahingehend zu Ermittlungserfolgen führen kann, dass Straftäter identifiziert werden konnten.

Diese Rechtsnorm bietet die Möglichkeit in besonders schwerwiegenden Situationen auf die Erkenntnisse aus dem Internet zugreifen zu dürfen. Die Befürchtung und Vorteil „die Polizei scannt damit ständig das Internet“, ungeachtet der rechtlichen Einschränkung schon allein aufgrund der mangelnden Kapazitäten und vorhandenen Leistungsbegrenzungen entgegnet werde. Der Schwerpunkt liegt im überwiegenden Fall auf einen eng definierten Bereich.

Die Besonderheit dieser Rechtsnorm liegt ohne Frage in der Herausgabe von biometrischen Daten an Dritte um aus deren Datenbeständen Hinweise zu weiteren Onlineauftritten der fraglichen Person zu erhalten. Aufgrund des Umfangs und der Bedeutung der personenbezogenen Daten wurde diese Maßnahme lediglich auch schwerwiegende bzw. nicht anders zu lösende Sachverhalte begrenzt. Dennoch gleicht diese Rechtsnorm das bisherige Missverhältnis aus, wonach die Polizei solche Dienste nicht nutzen durfte, während sie für jede Privatperson zur Verfügung steht.

Das Verbot der Echtzeitabgleiche scheint aktuell auch ein technisches Problem anzusprechen. Die GdP wünscht sich eine rechtliche Betrachtung, inwieweit der biometrische Abgleich bei Echtzeitübertragungen erfolgen darf, wenn der Abgleich im Polizeinetz und auf bestimmte Übertragungen begrenzt erfolgt (ohne Herausgabe der hier vorliegenden biometrischen Daten an Dritte).

Ferner wünscht sich die GdP inwieweit die biometrischen Daten für den Vergleich verändert werden dürfen (z.B. Alterung der betreffenden Person) und ob diese Veränderung einer Verschärfung oder Lockerung dieser Rechtsnorm bringt, da es sich nicht um die ursprünglich biometrischen Daten handelt.

Wozu Privatpersonen heutzutage schon in der Lage sind, sollte befugnistechisch der Polizei nicht vorenthalten werden. Dies betrifft insbesondere die gezielte Fahndung nach schweren Straftätern und Terroristen.

Aus diesem Grund begrüßt die GdP Sachsen diese Befugnis. Bezüglich des Einsatzes und notwendiger Software wird auf die Ausführungen zu § 62a verwiesen.

§ 66**Überwachung der Telekommunikation**

Die GdP Sachsen begrüßt ausdrücklich die Schaffung der Möglichkeit der Nutzung der sogenannten Quellen-TKÜ, weil sie ein wirkungsvolles Ermittlungsinstrument ist. Sie macht Inhalte zugänglich, die sonst durch moderne Verschlüsselung verborgen blieben.

Als Maßnahme erfasst sie die Kommunikation am Endgerät, also bevor sie Ende-zu-Ende-verschlüsselt wird (oder nach Entschlüsselung), unabhängig davon, ob sich der Nutzer aktiv für eine Verschlüsselung der Kommunikation entschieden hat. Fast alle gängigen Messengerdienste verschlüsseln von Haus aus die Kommunikation ihrer Anwender. Hinzukommt, dass erste Messengerdienste beginnen Post-Quantenverschlüsselung einzuführen, die auch eine nachträgliche Entschlüsselung erheblich erschweren oder gar verhindern.

Mittels der Quellen-TKÜ lassen sich Inhalte gewinnen, die durch klassische Abfangmethoden im Netz nicht zugänglich wären.

Problematisch sieht die GdP Sachsen die Höhe der Voraussetzung, welche nach Abs. 1 Nr. 1 ff vorliegen müssen, damit die Überwachung der Telekommunikation zugelassen ist. Im Regelfall der Fallkonstellationen Verwirklichen hier bereits Vorbereitungshandlung Straftatbestände z.B. im StGB, was zur Anwendung der StPO als Rechtsgrundlage hindeutet.

§ 71 Einsatz von unbemannten Luftfahrtsystemen

Abs. 1

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

1. Datenerhebung nach § 56,
2. offene Beobachtung und Aufzeichnung mittels Bildübertragung nach § 57 Absatz 1 bis 3 und Absatz 9,
3. Datenerhebung durch Observation und Einsatz technischer Mittel nach § 63 Absatz 1 und 2,
4. Datenerhebung durch Einsatz technischer Mittel in Wohnungen nach § 65 Absatz 1,
5. Datenerhebung durch Telekommunikationsüberwachung nach § 66 Absatz 1 und 2 sowie
6. Datenerhebung durch den verdeckten Einsatz technischer Mittel zur Standorterhebung nach § 68 Absatz 2.

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

Abs. 2

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

Abs. 3

Die Polizei kann im öffentlichen Verkehrsraum offen Übersichtsbildübertragungen anfertigen, wenn dies der Übersichtlichkeit der Lage zur Lenkung und Leitung von Verkehrsmaßnahmen und zur Dokumentation von Unglücks- oder Verkehrsunfällen im Einzelfall erforderlich ist. Eine Identifikation von Personen findet hierbei nicht statt.

Die GdP Sachsen regt durch das hinzufügen eines zusätzlichen Absatzes 3 an, dass unbemannte Luftfahrtsysteme auch zur Verkehrslenkung und -Leitung sowie zur Dokumentation größerer Verkehrs- oder Unglücksfällen im offenen im öffentlichen Verkehrsraum Bildübertragungen durchführen dürfen. Die alternativvariante wäre der kostspielige Einsatz ein Polizeihubschraubers.

§ 79c Training und Test von lernenden IT-Systemen

Die GdP Sachsen begrüßt die Schaffung dieser Rechtsnorm, aber sieht hier deutlichen Verbesserungsbedarf aufgrund mehrerer offenen Fragen.

Die Rechtsnorm ermöglicht die Herausgabe von personenbezogenen Daten aus den polizeilichen Datenbeständen zum Anlernen von Künstlichen Intelligenzen. Es erfolgt keine Begrenzung oder gesonderte Betrachtung der personenbezogenen Daten nach deren besonderer Bedeutung (z.B. Name, Geschlecht, Fingerabdrücke, DNA-Muster, andere Körpermerkmale, Familienverhältnisse).

Die Anonymisierung der Daten wird bevorzugt, jedoch ist auch die Weitergabe von pseudonymisierten Daten oder Klardaten möglich. Dabei wird nicht entschieden, ob der Datenempfänger Polizei, Auftragnehmer oder Dritter ist. Somit können im schlechtesten Fall Dritte ihre eigene Künstliche Intelligenz mit polizeilichen Klardaten trainieren und diese Künstliche Intelligenz anderen Kunden (auch Unternehmen, Privatpersonen, oder Behörden anderer Staaten) zur Verfügung stellen.

Die GdP Sachsen empfiehlt die Weitergabe der sehr sensiblen Daten anzupassen. Dabei sollte mit Abstand zur Polizei der Anonymisierungsgrad verstärkt werden. Demnach würde die sächsische Polizei oder andere Polizeibehörden in der Bundesrepublik mit Klardaten trainieren können, Auftragnehmer dürften mindestens pseudonymisierte Daten verwenden und Dritte lediglich anonymisierte Daten. Darüber hinaus sollte anhand des Anwendungsfalls betrachtet werden, inwieweit Klardaten oder pseudonymisierte Daten wirklich erforderlich sind.

Aktuell ist nicht bekannt, dass Trainingsdaten definitiv nicht aus einer Künstlichen Intelligenz extrahiert werden können. Die Trainingsdaten geben einen Toleranzbereich für das zu produzierende Ergebnis vor. Die Trainingsdaten liegen damit zwangsläufig in diesem Toleranzbereich. Dadurch ist eine (wenn auch sehr geringe) Wahrscheinlichkeit stets gegeben, dass diese Trainingsdaten aus einer Künstlichen Intelligenz erneut oder nur leicht abgewandelt generiert werden können.

Genauso ist unbekannt, inwiefern durch die polizeilichen Trainingsdaten Verzerrungen erzeugt oder verstärkt werden. Eine entsprechende Prüfung auf mögliche Benachteiligungen sollte intensiv direkt nach dem Training und vor dem Einsatz erfolgen. Ggf. ist der mit dem Training beauftragte Auftragnehmer und/oder Dritte zu verpflichten ein erneutes Training ohne polizeiliche Trainingsdaten durchzuführen, sofern solche Benachteiligungen festgestellt wurden.

Die Zwangsweise Löschung der polizeilichen Trainingsdaten durch denjenigen, der das Training durchführt ist, insbesondere bei Klardaten und pseudonymisierten Daten zu befürworten. Jedoch ist nicht geklärt, inwiefern diese Daten seitens der Polizei oder gar durch Auftragnehmer oder Dritte vorgehalten werden dürfen bzw. müssen, um ein erneutes Training für eine Aktualisierung der Künstlichen Intelligenz zu verwenden.

[1] <https://www.rola.com/de/insights/rola-und-chapsvision-schliessen-strategische-partnerschaft-fuer-europaeische-big-data-analyseplattform>

[2] <https://www.br.de/nachrichten/deutschland-welt/polizeisoftware-von-palantir-werden-alternativen-ignoriert,UzmaB7J>

§ 84a Öffentlichkeitsfahndung

Abs. 1 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

Abs. 2 Sonstige Fahndung

Personen dürfen, wenn es zur Durchführung erkennungsdienstlicher Maßnahmen nach diesem Gesetz oder nach § 81 b Abs. 1 Alt. 2 Strafprozessordnung (zum Zwecke des Erkennungsdienstes) erforderlich ist, zur Aufenthaltsermittlung ausgeschrieben werden, wenn der Aufenthalt der Person unbekannt ist.

Abs. 3 Fahndungshilfsmittel und Anordnung

Ausschreibungen zur Aufenthaltsermittlung dürfen in allen Fahndungshilfsmitteln der Polizei vorgenommen werden. Ausschreibungen zur Aufenthaltsermittlung bedürfen der Anordnung durch die Leiterin oder den Leiter der jeweiligen Polizeidienststelle oder von diesen beauftragten Bediensteten.

Es wird angeregt, dass die Maßnahme des § 84a durch zwei weitere Absätze ergänzt wird.

Die Ausschreibung von Personen zur Aufenthaltsermittlung zum Zweck der Durchführung von erkennungsdienstlichen Maßnahmen zu präventiven Zwecken würde eine Gesetzeslücke schließen und die polizeiliche Arbeit effektiveren. Eine Personenfahndung nach § 131a StPO zur Durchführung erkennungsdienstlicher Maßnahmen ist nur zum Zwecke des Strafverfahrens zulässig.

Eine Ausschreibung von Personen zur Aufenthaltsermittlung sollte nur durch eine Anordnung von Leiterinnen oder Leitern von Polizeidienststellen (Organisationseinheiten) möglich sein.

III. Stellungnahme zu weiteren Änderungsbedarfen

§ 3 Tätigwerden der Polizei für die Polizeibehörden oder andere Stellen

Wird die Polizei gemäß § 2 Absatz 3 tätig, trifft sie die erforderlichen **vorläufigen** 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.

Im Satz 1 sollte hinter „trifft die erforderlichen“ das Wort „vorläufigen“ eingefügt werden.

Die Polizei kann nur temporär die Aufgaben für andere Polizeibehörden oder andere Stellen wahrnehmen und die erforderlichen Maßnahmen treffen (Eilzuständigkeit). Die grundsätzliche Aufgabe bleibt aber in der originären Zuständigkeit der anderen Behörde. Insofern können die durch die Polizei getroffenen Maßnahmen lediglich vorläufigen Charakter haben bis die originär zuständige Behörde die Aufgabe übernimmt und ggf. die Maßnahme fortsetzt oder aufhebt.

§ 15 Identitätsfeststellungen, Prüfung von Berechtigungsscheinen

Abs. 2

Zur Feststellung der Identität kann die Polizei die erforderlichen Maßnahmen treffen.

Sie kann

1. die betroffene Person anhalten,
2. die betroffene Person nach ihren Personalien befragen,
3. verlangen, dass die betroffene Person mitgeführte Ausweispapiere zur Prüfung aushändigt,
4. die betroffene Person und von ihr mitgeführte Sachen nach Gegenständen durchsuchen, die zur Identitätsfeststellung dienen können,
5. die betroffene Person festhalten,
6. die betroffene Person zur Dienststelle bringen und
7. unter den Voraussetzungen des § 16 Absatz 2 Nummer 1 erkennungsdienstliche Maßnahmen durchführen.

Maßnahmen nach Satz 2 Nummer 4 bis 6 dürfen nur getroffen werden, wenn die Identität auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann oder wenn tatsächliche Anhaltspunkte dafür bestehen, dass Angaben unrichtig sind.

Es gelten die Grundsätze des § 27 Abs. 3 entsprechend.

Die GdP Sachsen regt an, den Satz „Es gelten die Grundsätze des § 27 Abs. 3 entsprechend“ am Ende des Absatzes als klarstellende Regelungen anzufügen, dass z.B. der gleichgeschlechtlichen Durchsuchung des § 27 Abs. 3 angewendet werden muss.

§ 18 Platzverweis

Die Polizei kann zur Abwehr einer Gefahr für die öffentliche Sicherheit **und Ordnung** eine Person vorübergehend von einem Ort verweisen oder ihr vorübergehend das Betreten eines Ortes verbieten (Platzverweisung).

Dies gilt insbesondere für Personen, die den Einsatz der Feuerwehr oder der Hilfs- und Rettungsdienste behindern.

Die GdP Sachsen regt an, dass in der Maßnahme des §18 der Begriff „**und Ordnung**“ als zweite Säule der Anwendung ergänzt wird.

Im Gegensatz zur öffentlichen Sicherheit, die sich auf den Schutz von Recht und Gesetz bezieht, geht es bei der öffentlichen Ordnung z.B. um die Einhaltung von Anstandsregeln und kulturell geprägten Erwartungen. Die öffentliche Ordnung ist die Gesamtheit der ungeschriebenen Verhaltensregeln in der Öffentlichkeit, deren Einhaltung als grundlegende Voraussetzung für ein geordnetes gesellschaftliches Zusammenleben gilt.

Sie umfasst soziale und ethische Normen, die nicht unbedingt in Gesetzen festgelegt sind, aber für ein friedliches Miteinander unerlässlich sind. Dazu gehören soziale Mindeststandards und Anstandsregeln, deren Einhaltung eine grundlegende Voraussetzung für ein funktionierendes Gemeinwesen ist.

Eine Störung der öffentlichen Ordnung liegt vor, wenn eine Handlung zwar noch keine ahndungsfähige Verwirklichung eines Tatbestandes Straftatbestandes oder einer Ordnungswidrigkeit darstellt, aber dennoch grundlegenden Verhaltensregeln nicht mehr gewährleistet werden. Sie betrifft vor allem das Verhalten im öffentlichen Raum wie Straßen, Parks und öffentliche Verkehrsmittel.

Beispiele für Störungen der öffentlichen Ordnung sind lautes Schreien oder Lärmen in der Öffentlichkeit, die Belästigung von Passanten z.B. durch unnötig schnelles Fahren durch Pfützen oder unzüchtiges Berühren (ohne sexuellen Hintergrund), das Stören einer Veranstaltung. Das Applaudieren, Gaffen oder Feiern an einer Unfallstelle wären weitere Beispiele.

§ 27 Durchsuchung und Untersuchung von Personen und Sachen

Abs. 1

Die Polizei kann eine Person durchsuchen, wenn

1. sie nach diesem Gesetz oder anderen Rechtsvorschriften festgehalten oder in Gewahrsam genommen werden kann,
2. Tatsachen die Annahme rechtfertigen, dass sie Tiere oder Sachen mit sich führt, die nach § 31 sichergestellt werden dürfen,
3. sie sich erkennbar in einem die freie Willensbildung ausschließendem Zustand oder sonst in hilfloser Lage befindet und dies zur Feststellung und zur Abwehr einer sie betreffenden Gefahr erforderlich ist,
4. sie sich an einem Ort im Sinne des § 15 Absatz 1 Satz 1 Nummer 2 aufhält,
5. sie sich in einem **Gebiet oder** einem Objekt im Sinne des § 15 Absatz 1 Satz 1 Nummer 3 oder in dessen unmittelbarer Nähe aufhält und Tatsachen die Annahme rechtfertigen, dass in oder an **diesen Objekten Orten** dieser Art Straftaten begangen werden sollen, oder
6. sie zur gezielten Kontrolle ausgeschrieben ist und die Maßnahme zur Verhütung der Straftat erforderlich ist.

Mit der sprachlichen Anpassung sollte klargestellt werden, dass Personen durchsucht werden können, wenn diese sich an einem der in § 15 Absatz 1 Satz 1 Nummer 3 genannten Orten aufhalten und wenn Tatsachen die Annahme rechtfertigen, dass in oder an diesen Orten Straftaten begangen werden sollten.

§ 31 Sicherstellung

Abs. 1

Die Polizei kann eine Sache sicherstellen,

1. ~~um eine gegenwärtige Gefahr abzuwehren~~ **zur Abwehr von Gefahren**,
2. um den Eigentümer oder rechtmäßigen Inhaber der tatsächlichen Gewalt vor Verlust oder Beschädigung der Sache zu schützen oder
3. wenn sie von einer Person mitgeführt wird, die nach diesem Gesetz oder anderen Rechtsvorschriften festgehalten wird, und die Sache verwendet werden kann, um

Die Anknüpfung an eine „**gegenwärtige Gefahr**“ ist bei den betreffenden Lebenssachverhalten nicht sachgerecht, da dieser Gefahrengrad im Unterschied zur konkreten Gefahr voraussetzt, dass das schädigende Ereignis bereits begonnen hat oder die Einwirkung unmittelbar oder in allernächster Zeit mit an Sicherheit grenzender Wahrscheinlichkeit bevorsteht (siehe Begriffsbestimmung in § 4 Nummer 3b) SächsPVDG).

Jedoch kann es Sachverhalte geben, wo die Gefahrenlage nicht so sehr im Zusammenhang mit der zeitlichen Nähe steht, vielmehr von der Wahrscheinlichkeit des Eintritts des Schadens abhängt. Beispielsweise könnte es Sachen bzw. gefährliche Gegenstände geben, die sich später als verbotene Gegenstände herausstellen oder auch später nicht herausgegeben werden können.

Notwendigkeit Einführung einer Online-Durchsuchung zur Gefahrenabwehr

Die GdP Sachsen regt an, dass die Folgemaßnahme zu § 66 (Überwachung der Telekommunikation) mit der Einführung einer Onlinedurchsuchung zur Gefahrenabwehr geschaffen wird.

Die Notwendigkeit der Online-Durchsuchung muss primär mit der Bekämpfung schwerer Kriminalität im digitalen Zeitalter verknüpft werden. Dabei kann die Einschreitschwelle zum § 66 mit einer konkreteren Gefahrenlage und Anwendungsbereichen erhöht sein.

Die gefährdende Handlungen werden zunehmend über verschlüsselte Kommunikation und Speichermedien sowie auf Computern vorgedacht und vorbereitet, so dass traditionelle Methoden wie die physische Wohnungsdurchsuchung oder Telefonüberwachung nicht mehr ausreichen.

Auf informationstechnischen Systemen (Computer, Smartphones, Onlinespeichern etc.) können umfangreiche Informationen gespeichert sein, die für die Verhinderung schwerer Straftaten, wie z.B. Terrorismus, Kinderpornografie oder organisierte Kriminalität, entscheidend sind.

Die sogenannte Online-Durchsuchung ermöglichen den Zugriff auf die Daten, bevor sie verschlüsselt werden oder nachdem sie entschlüsselt wurden, direkt auf dem Endgerät des Gefährders.

Die Online-Durchsuchung stellt einen intensiven Eingriff auf informationstechnischer Systeme dar, weswegen der Richtervorbehalt als wesentliche Voraussetzung gerechtfertigt ist.

Zusammenfassend lässt sich sagen, dass die Notwendigkeit der Online-Durchsuchung im Ringen zwischen einer effektiven Gefahrenabwehr (und Strafverfolgung) im digitalen Raum und dem Schutz fundamentaler Grundrechte in Abwägung gebracht werden muss. Die Rechtsprechung des BVerfG hat enge verfassungsrechtliche Grenzen für ihren Einsatz gesetzt, um die Verhältnismäßigkeit zu wahren, welche in der Ausgestaltung der Norm Grundlage sein können.

Artikel 2 Änderung des Sächsischen Polizeibehördengesetzes

zusätzliche Änderungen im Sächsischen Polizeibehördengesetz (SächsPBG)

§ 3

Begriffsbestimmung

Die Begriffsbestimmungen des § 4 des Sächsischen Polizeivollzugsdienstgesetzes vom 11. Mai 2019 (SächsGVBl. S. 358), in der jeweils geltenden Fassung, gelten entsprechend.

Die GdP Sachsen regt an, dass der Verweis auf § 4 SächsPVDG gestrichen werden sollte und dafür die für eine Polizeibehörde zutreffenden Begriffsbestimmungen eingefügt werden. Dies würde der Verbesserung der Rechtsanwendung des Polizeibehördenvertreters dienen. Begriffe, die für Polizeibehörden keine Rolle spielen, sollten dabei nicht übernommen werden.

§ 18

Identitätsfeststellung, Prüfung von Berechtigungsscheinen

Abs. 2

Die Polizeibehörden können die zur Feststellung der Identität erforderlichen Maßnahmen treffen. Sie können

1. den Betroffenen anhalten,
2. den Betroffenen nach seinen Personalien befragen,
3. verlangen, dass der Betroffene mitgeführte Ausweispapiere zur Prüfung aushändigt,
4. den Betroffenen und von ihm mitgeführte Sachen nach Gegenständen durchsuchen, die zur Identitätsfeststellung dienen können, oder
5. den Betroffenen festhalten **und bei Notwendigkeit ihn zu einer Dienststelle des Polizeivollzugsdienstes verbringen.**

Die GdP Sachsen regt mit der Einfügung der Formulierung „**und bei Notwendigkeit ihn zu einer Dienststelle des Polizeivollzugsdienstes verbringen.**“ in Nr. 5 an, dass für die Polizeibehörde die Möglichkeit geschaffen wird, Betroffene, deren Identität vor Ort nicht feststellbar ist, zu einem geschützten Ort zu verbringen.

§ 22

Gewahrsam

Abs. 1

Die Polizei kann eine Person in Gewahrsam nehmen, wenn

1. dies zum Schutz der Person gegen eine Gefahr für Leib oder Leben erforderlich ist, insbesondere weil die Person sich erkennbar in einem die freie Willensbestimmung ausschließenden Zustand oder sonst in hilfloser Lage befindet oder eine Selbsttötung droht,
2. dies unerlässlich ist, um die unmittelbar bevorstehende Begehung oder Fortsetzung ~~einer Straftat~~ **Rechtsverstößen eines Strafgesetzbuches oder einer Ordnungswidrigkeit von Ordnungswidrigkeitenrechtes mit** erheblicher Bedeutung zu verhindern,
3. dies unerlässlich ist, um vollziehbare Platzverweisungen, Aufenthaltsanordnungen, Kontaktverbote oder Wohnungsverweisungen durchzusetzen, oder
4. dies unerlässlich ist, um Maßnahmen der Identitätsfeststellung durchzuführen.

Die GdP Sachsen regt an, dass die Maßnahmengrundlagen nach §22 Abs. 1 Nr. 2 in nachfolgender Weise geändert wird. Anstelle der Formulierung „~~einer Straftat oder einer Ordnungswidrigkeit von~~“ wird „**Rechtsverstößen eines Strafgesetzbuches oder Ordnungswidrigkeitenrechtes mit**„. Mit dieser Änderung wird zum Ausdruck gebracht, dass auch strafunmündige (Kinder) und schuldunfähige Personen, welche keine Straftat begehen können sondern nur vorwerfbaren Handlungen, zur Unterbindung oder Verhinderung von Handlungen in Gewahrsam genommen werden können.

§ 25

Sicherstellung

(1) Die Polizeibehörden können eine Sache sicherstellen,

1. um eine ~~gegenwärtige Gefahr~~ abzuwehren, ...

Die GdP Sachsen regt an, dass der Gefahrenbegriff „~~gegenwärtige Gefahr~~“ durch den einfachen Gefahrenbegriff „**zur Abwehr von Gefahren**“ ersetzt wird.

Die Anknüpfung an eine gegenwärtige Gefahr ist bei den betreffenden Lebenssachverhalten nicht sachgerecht, da dieser Gefahrengrad im Unterschied zur konkreten Gefahr voraussetzt, dass das schädigende Ereignis bereits begonnen hat oder die Einwirkung unmittelbar oder in allernächster Zeit mit an Sicherheit grenzender Wahrscheinlichkeit bevorsteht (siehe Begriffsbestimmung in § 4 Nummer 3b) SächsPVDG). Jedoch kann es Sachverhalte geben, wo die Gefahrenlage nicht so sehr im Zusammenhang mit der zeitlichen Nähe steht, vielmehr von der Wahrscheinlichkeit des Eintritts des Schadens abhängt. Beispielsweise könnte es Sachen bzw. gefährliche Gegenstände geben, die sich später als verbotene Gegenstände herausstellen oder auch später nicht herausgegeben werden können.

§ 26**Verwahrung**

Abs. 2

~~Betroffenen ist eine Bescheinigung auszustellen, die den Grund der Sicherstellung erkennen lässt und die sichergestellte Sache bezeichnet.~~

Dem Betroffenen ist der Grund der Sicherstellung zu nennen und, wenn möglich, unverzüglich eine Bescheinigung der sichergestellten Sachen, die den Grund der Sicherstellung bezeichnet, auszustellen.

Die GdP Sachsen regt an, dass Satz 1 durch den o. g. Satz ersetzt werden sollte.

Dem Betroffenen sollte auf jeden Fall der Grund der Sicherstellung genannt werden. In vielen Fällen ist es jedoch nicht möglich, schon vor Ort eine Bescheinigung auszustellen, in der der Grund der Sicherstellung aufgezeigt wird.

§ 30**Datenerhebung durch den Einsatz technischer Mittel zur Bildaufnahme und -aufzeichnung**

Abs. 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 **bedeutende** 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.

Durch die GdP Sachsen wird angeregt, dass vor der Wortgruppe „**Sach- und Vermögenswerte**“ das Wort „**bedeutende**“ eingefügt wird. Das Anfertigen von Bildaufzeichnungen im öffentlichen Raum, gerade mit hohem Personenaufkommen, sollte schon vom Tatbestand her angemessen sein (Verhältnismäßigkeit).

Sollten Sie noch Fragen haben, stehe ich Ihnen gern zur Verfügung.

Mit freundlichen Grüßen



Jan Krumlovsky

-Landesvorsitzender-



Sächsischer Richterverein

Verein der Richter und Staatsanwälte in Sachsen

Sächsischer Richterverein – Der Landesvorsitzende
Dr. Alexander Brech, Hans-Oster-Str. 4, 01099 Dresden

Sächsisches Staatsministerium
des Innern
Referat Recht der Polizei
Anhoerung.SaechsPVDG@smi.sachsen.de

Der Landesvorsitzende

Dr. Alexander Brech
c/o Sozialgericht Dresden
Hans-Oster-Str. 4, 01099 Dresden
Telefon: 0351/446-5345
E-Mail: alexander.brech@sgdd.justiz.sachsen.de

Dresden, 14. November 2025

Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG)

hier: Stellungnahme zum Referentenentwurf

Ihr Schreiben vom 6. Oktober 2025, Az.: 36-2002/25/14

Sehr geehrte Damen und Herren,

der Sächsische Richterverein e.V. – Verband der Richter und Staatsanwälte in Sachsen – bedankt sich für die Gelegenheit zur Stellungnahme, die ich im Folgenden gerne nutze.

Unser Verband begrüßt die Zielsetzung des Referentenentwurfs, die verfassungsgerichtliche Rechtsprechung konsequent umzusetzen sowie die Befugnisse der Polizei auf klare, bestimmte und verlässliche gesetzliche Ermächtigungsgrundlagen zu stützen. Hierdurch wird die Rechtssicherheit sowohl für die handelnden Polizeibediensteten als auch für die betroffenen Bürgerinnen und Bürger erhöht. Der Sächsische Richterverein unterstützt die mit dem Entwurf verbundene Einführung zusätzlicher Richtervorbehalte, leisten diese doch einen wichtigen Beitrag zur rechtsstaatlichen Kontrolle polizeilichen Handelns. Soweit Belange der Justiz unmittelbar betroffen sind, erscheinen aus unserer Sicht insbesondere folgende Punkte hervorhebenswert:

1. Berücksichtigung personeller Kapazitäten der Justiz

In Anbetracht des auch in der sächsischen Justiz laufenden Generationenwechsels und der weiterhin erheblichen Arbeitsbelastung der Gerichte sollte bei der Einführung zusätzlicher Richtervorbehalte noch stärker Rücksicht auf die personellen Kapazitäten der Justiz genommen werden, als dies im aktuellen Entwurf der Fall ist. Denn die praktische Wirksamkeit von Richtervorhalten als Instrumentarium staatlicher Kontrolle hängt auch wesentlich davon ab, dass die betroffenen Gerichte personell in die Lage versetzt werden, diese zusätzlichen Aufgaben zeitnah und inhaltlich fundiert wahrzunehmen.

Der Sächsische Richterverein bittet daher dringend darum, den zusätzlichen personellen und organisatorischen Aufwand noch stärker zu berücksichtigen und sich dafür einzusetzen, die Einführung weiterer Richtervorbehalte mit einer entsprechenden personellen Stärkung der Justiz zu flankieren.

2. Zentralisierung der Richtervorbehalte im SächsPVDG

Der Sächsische Richterverein regt an, sämtliche Richtervorbehalte im SächsPVDG – nicht zuletzt im Interesse der Übersichtlichkeit, Verständlichkeit und besseren Lesbarkeit des Gesetzes – in einer eigenen Vorschrift zusammenzufassen. Ein entsprechendes Modell lässt sich etwa Art. 94 des Bayerischen Polizeiaufgabengesetzes (PAG) entnehmen, wo sämtliche richterlichen Zuständigkeiten und Verfahren übersichtlich gebündelt dargestellt werden. Eine derartige Regelung würde die praktische Handhabung des SächsPVDG erleichtern, zugleich zu einer einheitlichen Verfahrenspraxis beitragen und nicht zuletzt die hohe Bedeutung der Richtervorbehalte als Instrumentarium staatlicher Kontrolle noch stärker herausstellen.

3. Redaktionelle Anpassung von § 21 Abs. 3 Satz 1 SächsPVDG-E

Nach dem Entwurf soll § 21 Abs. 3 Satz 1 SächsPVDG wie folgt lauten: „Maßnahmen nach Absatz 2 bedürfen der Anordnung durch das Amtsgericht auf Antrag der Polizei.“ Eine ausdrückliche Benennung des Amtsgerichts erscheint an dieser Stelle entbehrlich, da nach § 73 Abs. 2 Satz 1 SächsPVDG (Artikel I Ziffer 23 des Entwurfs) bereits vorgesehen ist, dass für alle richterlichen Maßnahmen nach diesem Gesetz das Amtsgericht zuständig ist. Es wird daher vorgeschlagen, in Anlehnung an den Wortlaut von § 61 Abs. 3 SächsPVDG (Artikel I Ziffer 15 des Entwurfs) und § 62b Abs. 3 SächsPVDG (Artikel I Ziffer 16 des Entwurfs) auch in § 21 Abs. 3 Satz 1 SächsPVDG lediglich zu formulieren: „Maßnahmen nach Absatz 2 bedürfen der richterlichen Anordnung auf Antrag der Polizei.“

Für Rückfragen und Erörterungen stehen wir jederzeit gerne auch persönlich zur Verfügung.

Mit freundlichen Grüßen

gez. Dr. Alexander Brech
Landesvorsitzender

Der Sächsische Richterverein e.V. - Verein der Richter und Staatsanwälte in Sachsen (SRV) ist der sächsische Landesverband des Deutschen Richterbundes (DRB). Er gehört zu den Gründungsmitgliedern des DRB und ist 1907 gegründet worden. Im Zuge der Auflösung des DRB 1933 hat sich auch der SRV aufgelöst. Er ist nach der friedlichen Revolution 1990/91 wiederbegründet worden. Der DRB ist mit rund 18.500 Mitgliedern in 25 Landes- und Fachverbänden der mit Abstand größte Berufsverband der Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte in Deutschland. Der SRV selbst hat über 500 Mitglieder.

Fraktion BÜNDNIS 90/DIE GRÜNEN • Sächsischer Landtag • 01067 Dresden

Sächsische Staatskanzlei
Chef der Staatskanzlei
Herr Dr. Andreas Handschuh
01095 Dresden

Franziska Schubert
Fraktionsvorsitzende

Bernhard-von-Lindenau-Platz 1
01067 Dresden

Telefon: 0351 493 48 12
Telefax: 0351 / 493 48 21

Franziska.schubert@slt.sachsen.de

Dresden, den 9. Dezember 2025

**SächsKIV: Stellungnahme Fraktion BÜNDNIS 90/DIE GRÜNEN zum
Referentenentwurf des Gesetzes zur Änderung polizeirechtlicher Vorschriften**

Sehr geehrter Herr Chef der Staatskanzlei,
sehr geehrter Herr Dr. Handschuh,

vielen Dank für die Zuleitung des Entwurfes des Gesetzes zur Änderung polizeirechtlicher Vorschriften und anderer Vorschriften, welcher uns durch den Landtagspräsidenten am 02. Oktober 2025 im Zuge der Sächsischen Konsultations- und Informationsvereinbarung (SächsKIV) übermittelt wurde.

Gemäß Ziff. I. 4 Satz 3 SächsKIV nimmt die Fraktion BÜNDNIS 90/DIE GRÜNEN hierzu wie folgt Stellung:

Der sächsische Gesetzgeber ist aufgrund des Urteils des Verfassungsgerichtshofs des Freistaates Sachsen vom 25.01.2024 dazu verpflichtet, bis zum 30. Juni 2026 nach Maßgabe der im Urteil genannten Gründe ergänzende Regelungen zu einzelnen Vorschriften des Sächsischen Polizeivollzugsdienstgesetzes und des Sächsischen Polizeibehördengesetzes zu treffen.

In dem nun vorliegenden Referentenentwurf sind jedoch nicht nur die in diesem Zusammenhang zu reformierenden Vorschriften mit den entsprechenden Änderungen enthalten, sondern auch viele neue Befugnisse und andere weitreichende Änderungen.

In diesem Zusammenhang weist die Fraktion BÜNDNIS 90/DIE GRÜNEN grundsätzlich darauf hin, dass sie die zu beobachtende Verschärfung polizeirechtlicher Vorschriften sowie die Trends zur Ausweitung polizeilicher Befugnisse und die Etablierung neuer Instrumente für die Polizei sehr kritisch sieht. Dies betrifft im nun vorgelegten Referentenentwurf insbesondere die flächendeckende Ausstattung mit Tasern, den Einsatz von Bodycams in Wohnungen, die Möglichkeiten zur KI-gesteuerten Datenanalyse und die Befugnis zur biometrischen Echtzeit-Fernidentifizierung, sowie die KI-gesteuerte Datenanalyse zur Gewinnung neuer Erkenntnisse durch die automatisierte Zusammenführung, Verknüpfung, Aufbereitung und Auswertung von gespeicherten personenbezogenen Daten, die Befugnis zum nachträglichen Abgleich von Bildern und Stimmen mit öffentlich zugänglichen Quellen aus dem Internet mittels einer automatisierten Anwendung und die Quellen-Telekommunikationsüberwachung.

Erweiterte Befugnisse, gesenkte Eingriffsschwellen und die Einführung neuer Instrumente wurden in im Referentenentwurf damit begründet, dass neben den Vorgaben des Verfassungsgerichtshofes auch in zehn anderen Bundesländern die Polizeigesetze geändert wurden oder sich gerade im Änderungsprozess befinden und sich die Minderheitsregierung in Sachsen mit ihrem nun vorgelegten Vorschlag auf Augenhöhe mit den anderen Bundesländern befände.

Für BÜNDNIS 90/DIE GRÜNEN gilt: Die Sicherheit der Menschen ist ein hohes und ohne Frage zu schützendes Gut. Sie darf jedoch nicht auf Kosten von Freiheit, Rechtsstaatlichkeit und Vertrauen in die staatlichen Institutionen gehen. Die Freiheit darf nie zum Schutz der Freiheit aufgegeben werden, das ist ein Widerspruch in sich. Und auch die Vorstellung, durch immer weitergehende Befugnisse immer mehr Sicherheit schaffen zu können, ist trügerisch, denn unabhängig von der Frage, wie effektiv bestimmte Maßnahmen zur Erreichung dieses Ziels überhaupt sind bzw. sein können, entstehen durch weitergehende Befugnisse neue Unsicherheiten wie die Angst vor willkürlichen Eingriffen, die Selbstzensur im öffentlichen Raum, der Verlust von Vertrauen in öffentliche und auch nichtöffentliche Institutionen und die Angst vor dem Missbrauch dieser Befugnisse.

Sicherheit entsteht nicht durch die Überwachung von Menschen und immer weitere Befugnisse für staatliche Institutionen. Sie entsteht dadurch, dass Menschen sich frei entfalten können, ohne Angst vor Gewalt, Diskriminierung oder Überwachung egal durch welche Akteure. Sie entsteht durch gesellschaftlichen Zusammenhalt und eine Polizei, die Partnerin für die Menschen ist und deren Vertrauen genießt.

Polizeirechtliche Verschärfungen und erweiterte Befugnisse bedeuten immer auch verstärkte Eingriffe in Grundrechte der Bürger*innen. Diese mögen erst einmal teilweise ungefährlich klingen, in ihrer Tragweite nicht immer für alle absehbar sein und am Ende bleibt jeder Eingriff auch immer eine Einzelfallentscheidung. Doch aus Einzelfallentscheidungen und Ausnahmen können Routinen werden. So können sich Grenzen immer weiter verschieben und Eingriffe immer normaler werden. Zudem ist mit Blick auf die Befugnisse der Ermittlungsbehörden zu konstatieren, dass bestehende – für sich genommen hinreichend eingegrenzte – später immer mehr ausgeweitet werden. Auch deshalb sollten insbesondere neue technische Instrumente und Befugnisse mit Zurückhaltung eingeführt werden.

All diese Überlegungen sehen wir in dem vorgelegten Referentenentwurf nicht abgebildet, im Gegenteil – die neu geschaffenen Befugnisse gehen deutlich zu weit, ohne dass dabei ein Bewusstsein, geschweige denn eine Absicherung hinsichtlich der damit zugleich verbundenen Risiken zum Vorschein kommt. Es fehlt an vielen Stellen an einer erkennbaren Abwägung zwischen der tatsächlichen Notwendigkeit neuer Befugnisse und deren Wirkung auf die Grundrechte der Bürgerinnen und Bürger in einer Gesamtbetrachtung.

Darüber hinaus erschließt sich auch nicht, warum gerade vor der oben beschriebenen erkennbaren Tendenz, Befugnisse der Polizei stets erweitern zu wollen und polizeirechtliche Vorschriften generell zu verschärfen, den mehrfach deutlich geäußerten Forderungen der kommunalen Ebene, eine Rechtsgrundlage für Maßnahmen zur Stärkung der Sicherheit öffentlicher Veranstaltungen zu schaffen, entgegen der Ankündigung des Sächsischen Staatsministeriums des Innern, nicht entsprochen wurde. Die Fraktion BÜNDNIS 90/DIE GRÜNEN hält es für dringend notwendig hier Klarheit zu schaffen, um die Kommunen angemessen entlasten zu können und parallel für den notwendigen Schutz auf Veranstaltungen sorgen zu können.

Parallel zu den oben geäußerten Bedenken hinsichtlich der grundsätzlichen Verschärfung polizeirechtlicher Regelungen muss selbstverständlich auch darauf geachtet werden, dass die Polizei auf dem aktuellen Stand der Technik bleibt, um für unser aller Sicherheit und Ordnung sorgen zu können und auch unsere Regelungswerke in diesem Punkt den Anschluss nicht verlieren. Die im Rahmen der Novellierung geschaffene Rechtsgrundlage für die Polizei

technische Mittel gegen unbemannte Fahrzeugsysteme/Drohnen einzusetzen begrüßt die Fraktion BÜNDNIS 90/DIE GRÜNEN deshalb grundsätzlich, auch hier stellen sich jedoch technische und rechtliche Fragen.

Darüber hinaus stoßen viele andere geplante Vorschriften auf Unverständnis, teilweise sind diese nach hiesiger Auffassung verfassungswidrig oder führen zu einer unverhältnismäßigen Verschiebung der Balance zwischen Sicherheit und Freiheitsrechten zu Ungunsten letzterer.

Zu einzelnen (ausgewählten) Vorschriften:

1) Nr. 4: § 12a Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme

Die Vorschrift soll der Polizei in Satz 1 die Möglichkeit geben, zur Abwehr einer Gefahr, die von unbemannten Fahrzeugsystemen ausgeht, die an Land, in der Luft oder zu Wasser betrieben werden, technische Mittel gegen das System, dessen Steuerungseinheit oder Steuerungsverbindung einzusetzen. Nach der Gesetzesbegründung zu § 12a darf die Polizei auch durch physische Mittel auf die unbemannten Fahrzeugsysteme einwirken. Dies findet sich in der Vorschrift allerdings nicht wieder, der Wortlaut spricht ausschließlich von „technischen Mitteln gegen das System“. Hier sollte klargestellt werden, was der Polizei für Mittel an die Hand gegeben werden sollen, um die Norm für die Einsatzkräfte handhabbar zu gestalten.

Darüber hinaus ermöglicht Satz 2 den Einsatz technischer Mittel zur Erkennung einer Gefahr. Zwar bezieht sich Satz 2 auf Satz 1 und damit auf die Gefahrenabwehr von unbemannten Fahrzeugsystemen, diese Befugnis ist jedoch geeignet, die vollumfängliche und durchgehende Überwachung an Land, in der Luft und zu Wasser zu begründen und auch in der Gesetzesbegründung nicht näher ausgestaltet. Um Missbrauch zu verhindern sollten entsprechende und angemessene Anordnungs-, Kontroll-, Berichts-, Evaluations- und Aufhebungspflichten aufgenommen werden.

2) Nr. 5: § 15 Identitätsfeststellung, Prüfung von Berechtigungsscheinen

Die Änderung der Nummer 5 erschließt sich nicht. Sie ermöglicht die Identitätsfeststellung, wenn sich eine Person in einem Fahrzeug befindet, das zur gezielten Kontrolle ausgeschrieben ist und tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme zur Abwehr einer Gefahr erforderlich ist. § 15 Nummer 1 ermöglicht bereits die Identitätsfeststellung einer Person unabhängig vom Ort oder Gegenstand an/in dem sie sich aufhält. Der gesonderte Anwendungsbereich ergibt sich auch nicht aus der Gesetzesbegründung. Hier sollte mindestens klargestellt werden, warum die Änderung erfolgen sollen.

3) Nr. 6: § 19 Maßnahmen zum Schutz vor häuslicher Gewalt und sonstigen Nachstellungen

Dass Maßnahmen zum Schutz vor häuslicher Gewalt und sonstigen Nachstellungen mit in die Novellierung aufgenommen wurden und explizit auch als solche benannt sind wird grundsätzlich begrüßt.

Durch die generelle Absenkung der Eingriffsschwelle von einer gegenwärtigen auf eine konkrete Gefahr sehen wir allerdings in bestimmten Fällen die Gefahr von Anwendungsschwierigkeiten. Denn mit den in der Vorschrift genannten Maßnahmenmöglichkeiten gehen auch erhebliche Grundrechtseingriffe einher. Sofern in die Verletzlichkeit der Wohnung gemäß Art. 30 SächsVerf eingegriffen wird, in dem Einsatzkräfte beispielsweise in die Wohnung eindringen, ist dies gemäß Art. 30 Abs. 3 SächsVerf nur zur

Abwehr einer dringenden Gefahr möglich. Hier sollte die Vorschrift an eine solche Situation entsprechend angepasst werden, um Anwendungsschwierigkeiten zu verhindern.

Darüber hinaus halten wir die Frist in § 19 Absatz 1 Satz 3 für zu kurz. Hiernach enden die Maßnahmen des Absatzes 1 mit dem Ablauf des 14. Tages nach ihrer Anordnung, soweit nicht die Polizei im Einzelfall eine kürzere Frist festlegt. Stellt die gefährdete Person während dieser Dauer einen Antrag nach dem Gewaltschutzgesetz, enden die Maßnahmen mit dem Tag der gerichtlichen Entscheidung oder des gerichtlichen Vergleichs, spätestens jedoch mit Ablauf des 14. Kalendertages nach dem Ende der nach Satz 3 bestimmten Dauer. Betroffene brauchen nach Taten, die Maßnahmen nach § 19 Absatz 1 rechtfertigen, genug Zeit um zu handeln. Der gesetzlich vorgegebene Zeitrahmen muss deshalb berücksichtigen, dass Betroffene nach häuslicher Gewalt zunächst einmal ausreichend Zeit benötigen, um sich emotional zu stabilisieren bzw. ggf. auch durch professionelle Hilfe stabilisieren zu lassen und organisatorische, finanzielle und rechtliche Fragen zu klären.

Das beinhaltet zunächst einmal Zeit für die Betroffenen, um ansatzweise verstehen zu können was passiert ist und anfangen zu können, das Geschehene zu verarbeiten.

Sollte anschließend professionelle Hilfe durch Psychiater*innen oder Psycholog*innen in Anspruch genommen werden, ist die Versorgungslage in Deutschland zum aktuellen Zeitpunkt nicht so ausgestaltet, dass eine Versorgung jederzeit bzw. kurzfristig möglich ist. Der Patient*innenservice 116117 gibt an, dass sie innerhalb einer Woche einen Termin vermitteln, der dann höchstens vier Wochen in der Zukunft, bei einer Akutbehandlung maximal zwei Wochen in der Zukunft liegen darf.

Es muss außerdem ausreichend Zeit eingeplant werden für sachgerechte Beratungen in Fachberatungsstellen, ggf. Frauenhäusern und durch Anwälte*innen. Darüber hinaus müssen organisatorische und finanzielle Fragen geklärt werden und genug Zeit bleiben, um über längerfristige Schutzmaßnahmen nachzudenken.

All diese Dinge lassen sich angesichts der angespannten medizinischen und psychiatrischen/psychologischen Versorgungslage, der angespannten Situation der Beratungsstellen und Frauenhäuser, des angespannten Wohnungsmarktes und der psychischen und ggf. körperlichen Belastung unter der Betroffene nach häuslicher Gewalt leiden, nicht innerhalb von 14 Tagen (und ggf. auch einem kürzeren Zeitraum) verwirklichen.

Hinzu kommt, dass das Risiko einer Aggressivitäts- und Gewaltsteigerung der Täter umso höher ist, je kürzer der Zeitraum der Maßnahmen des Absatzes 1 bemessen ist.

In Gesamtschau dieser Umstände halten wir eine Frist von 28 Tagen für angemessen und notwendig.

4) Nr. 10: Änderung § 40 IV Ausweitung des Einsatzes von Vorrichtungen für den Abschuss besonderer Formen von Projektilen (Taser)

Die Vorschrift ermöglicht den flächendeckenden Einsatz von Tasern bei der Polizei. Bisher war dieser den Spezialkräften vorbehalten.

Laut Gesetzesbegründung stellen Taser das mildere Mittel zum Schusswaffengebrauch dar, weil sie ein geringeres Verletzungsrisiko mit sich bringen. Damit dürften sie auch nur in den Fällen einsetzbar sein, in denen auch ein Schusswaffengebrauch zulässig ist. So lässt sich die Vorschrift mit Blick auf die Gesetzesbegründung auslegen. Die im Referentenentwurf nicht vorgesehenen Änderungen der Vorschriften des Sächsischen PVDG über den Schusswaffengebrauch (§§ 43 ff.) lassen allerdings auch die Auslegung zu, dass die Schwelle

unterhalb des Schusswaffengebrauchs anzusiedeln ist. Insofern ist aktuell unklar, wann die Vorschrift den Einsatz des Tasers ermöglichen soll.

Auch die Annahme, dass Taser mildere Mittel sind, dürfte allenfalls auf gänzlich gesunde Menschen zutreffen. Schwangere, psychisch Erkrankte (durch ein ggf. fehlendes Verständnis des Einsatzmittels und ein dadurch eskalierendes Potenzial), unter Drogeneinfluss stehende Menschen und Menschen mit Vorerkrankungen sind beim Einsatz von Tasern stark gefährdet.

Diese Erkrankungen, Gesundheitszustände und körperlichen Zustände sind regelmäßig nach außen nicht erkennbar. Schwangerschaften sind häufig erst in späten Stadien und psychische Erkrankungen und Drogenkonsum nur teilweise überhaupt nach außen sichtbar. Vorerkrankungen wie bspw. Herz-Kreislauf-Erkrankungen, unter denen mittlerweile ein großer Teil der Gesellschaft leidet, werden wohl fast nie für Einsatzkräfte erkennbar sein und zwar vor allem nicht in Gefahrensituationen, in denen ein Schusswaffengebrauch zulässig wäre, also regelmäßig sehr dynamischen Einsatzsituationen, die eine schnelle Entscheidung erforderlich machen.

Aufgrund der Gefährlichkeit des Einsatzmittels für u.a. diese Personengruppen stellt der Taser dann kein milderes Mittel mehr dar, führt aber dazu, dass Einsatzkräfte mehr Einsatzmittel an sich tragen, zwischen denen sie sich in einer akuten Gefahrensituation entscheiden müssen. Dies kann im Worst-Case-Szenario dazu führen, dass sich eine Einsatzkraft für die Schusswaffe entscheidet und eine andere zeitgleich zum Einsatz des Tasers wie der erst kürzlich medial präsente Einsatz in Bochum zeigen könnte, bei dem ein gehörloses Mädchen lebensgefährlich verletzt wurde.

Da überdies keine Vollausrüstung aller Polizeibediensteten geplant ist, hängt in der Praxis die Frage, ob statt der Schusswaffe der Taser eingesetzt wird, für das polizeiliche Gegenüber faktisch vom Zufall ab.

Aus den genannten Gründen lehnt die Fraktion BÜNDNIS 90/DIE GRÜNEN den Taser als Einsatzmittel jenseits der Spezialeinsatzkräfte ab.

5) Nr. 13: § 57 Offener Einsatz technischer Mittel zur Bild- und Tonaufnahme und -aufzeichnung

Absatz 4 ermöglicht den Einsatz von Bodycams jetzt auch in Wohnungen. Begründet wird die Erweiterung des Bodycam-Einsatzes mit der deeskalierenden Wirkung von Bodycams zum Schutz der Einsatzkräfte.

Dies stellt einen Eingriff in die grundrechtlich geschützte Unverletzlichkeit der Wohnung dar (Art. 13 Absatz 7 GG, Art. 30 Absatz 1 SächsVerf). Solche Eingriffe dürfen nur zur Abwehr einer dringenden Gefahr für Leib oder Leben erfolgen. § 57 Absatz 4 Satz 2 erlaubt das Pre-Recording in Wohnungen allerdings bereits dann, soweit und solange dies mit hinreichender Wahrscheinlichkeit zur Abwehr einer dringenden Gefahr für Leib oder Leben der eigenen oder einer dritten Person erforderlich ist. Die Anforderung an die Wahrscheinlichkeit des Schadenseintritts ist so weder im Grundgesetz, noch in der Sächsischen Verfassung vorgesehen. Es darf nur zur Abwehr einer dringenden Gefahr eingegriffen werden. Damit verstößt diese Vorschrift gegen die verfassungsrechtlichen Vorgaben. Sofern die Begründung ausführt, die Dringlichkeit der Gefahr bezöge sich nicht auf die Wahrscheinlichkeit des Schadenseintritts, sondern auf den Umfang des drohenden Schadens, erschließt sich diese Aussage nicht und verkennt die notwendige Anknüpfung an eine reale Gefahrenschwelle.

Darüber hinaus halten wir den Einsatz von Bodycams in Wohnungen grundsätzlich für unverhältnismäßig. Laut Gesetzesbegründung ist Zweck des Einsatzes in Wohnungen der Schutz der Einsatzkräfte aufgrund der deeskalierenden Wirkung. Dies mag grundsätzlich ein

legitimer Zweck sein, sowohl die Erforderlichkeit, als auch die Angemessenheit stellen wir allerdings stark in Frage.

Es vertreten mittlerweile viele die Auffassung, dass Bodycams nicht per se eine deeskalierende Wirkung zugeschrieben werden kann. Auch die letzten Evaluationen zum grundsätzlichen Einsatz von Bodycams in Sachsen haben gezeigt, dass sich keine eindeutigen Schlüsse auf eine generalpräventive Wirkung von Bodycams ziehen lassen können oder dass ein pauschaler Beitrag zur Deeskalation geleistet würde. Insbesondere auch bei alkoholisierten oder unter Betäubungsmitteln stehenden Personen wird eine deeskalierende Wirkung stark bezweifelt. Eine eventuell mögliche, wenn auch anscheinend nicht nachweisbare, deeskalierende Wirkung kann sich aber jedenfalls dann zwangsläufig endgültig nicht entfalten, wenn die betroffenen Personen vom Einsatz der Bodycams nichts wissen (wie in Absatz 7 unter bestimmten Voraussetzungen als Möglichkeit vorgesehen).

Als milderes Mittel stünde der Einsatz von mehr Personal bei Situationen häuslicher Gewalt zur Verfügung, der aufgrund mangelnder Aufzeichnung des höchstpersönlichen Lebensraums der Menschen grundrechtsschonender wäre und zudem auch sehr viel wirksamer, weil diese viel eher in der Lage sind, sich selbst als Einsatzkräfte und Dritte jeweils zu schützen.

Die Wahrscheinlichkeit, dass mittels Bodycams Einsatzkräfte besser geschützt würden ist mangels einer nachgewiesenen deeskalierenden Wirkung sehr niedrig, wenn überhaupt vorhanden. Dem gegenüber steht ein schwerer Eingriff in die Grundrechte der betroffenen Personen.

Absatz 6 enthält Regelungen zum Kernbereich, wenn dieser durch den Einsatz von Bodycams betroffen ist. Dies wird so auch in der Gesetzesbegründung beschrieben. Der Zusammenhang mit dem Einsatz von Bodycams muss herausgenommen werden, da die Verletzung des Kernbereichs privater Lebensgestaltung immer und überall verboten ist.

Aus Sicht der BÜNDNISGRÜNEN Fraktion wären allerhöchstens Anpassungen denkbar, die den Begriff des Wohnraumes konkretisieren und Regelungen, dass sich automatisch beim Einsatz der Schusswaffe die Bodycam anschaltet.

Absatz 9 enthält eine Rechtsgrundlage zur präventiven Überwachung von fahrzeugführenden Personen im öffentlichen Verkehrsraum zur Aufdeckung der Nutzung elektronischer Geräte am Steuer (§ 23 Absatz 1a StVO) mittels technischer Mittel zur Bildübertragung und -aufzeichnung. Diese Vorschrift halten wir für eindeutig verfassungswidrig.

Der Sächsische Verfassungsgerichtshof hat in dem Urteil zu dem aktuell geltenden Sächsischen PVDG klargestellt, dass keine Rechtsgrundlagen geschaffen werden dürfen, die Überwachungsmaßnahmen vorsehen, um Straftaten abzuwehren, die bloße Rechtsgutsgefährdungen sanktionieren. § 57 Absatz 9 dient nicht nur der Überwachung des öffentlichen Verkehrsraums zur Verhütung von Verstößen gegen eine Ordnungswidrigkeit (also nicht einmal zur Abwehr einer Straftat), sondern auch zur Verhütung von Verstößen gegen einen Ordnungswidrigkeitstatbestand, der eine bloße abstrakte Gefährdung sanktioniert.

Ein Verstoß gegen eine Ordnungswidrigkeit soll hier dazu dienen, den öffentlichen Verkehrsraum zu überwachen und damit in eine unüberschaubar große Anzahl von Grundrechten der betroffenen Verkehrsteilnehmer*innen einzugreifen. Und zwar von allen, die sich an den entsprechenden Verkehrsknotenpunkten oder Streckenabschnitten aufhalten und nicht wie in der Gesetzesbegründung aufgeführt nur von den Personen, die infolge des Begehens des Ordnungswidrigkeitstatbestandes abstrakt den Straßenverkehr gefährden. Auch hier geht der Wortlaut der Vorschrift und die zugehörige Begründung wieder auseinander. Nach Absatz 9 Satz 3 sind die Bilddaten sofort nach Beendigung der Maßnahme zu löschen, aus denen sich kein Hinweis auf einen Verstoß gegen § 23 Absatz 1a StVO ergibt. Dies

bedeutet zwangsläufig, dass alle Verkehrsteilnehmer*innen erst einmal überwacht werden und damit in diesem Moment in ihre Grundrechte eingegriffen wird. Es erschließt sich außerdem auch nicht, was mit „Beendigung der Maßnahme“ gemeint ist, das ist nirgendwo näher konkretisiert.

Rein gesetzgebungstechnisch finden wir es schließlich angesichts der mit der Vorschrift einhergehenden schweren Grundrechtseingriffe auch der Gesellschaft gegenüber verantwortungslos, ein solches Vorhaben als Absatz 9 in § 57 aufzunehmen. Die Regeln, die die Gesetzgebung entwirft, sollen als Grundlage für unser aller Zusammenleben dienen und wir sind es den Menschen schuldig, Gesetze so zu schreiben, dass sie für alle verständlich sind und alle relativ einfach und schnell die Dinge finden, die sie betreffen (können). Die Befugnisnorm, die mit § 57 Absatz 9 geschaffen werden soll, betrifft tendenziell alle Verkehrsteilnehmer*innen in Sachsen und gehört deshalb nicht ans Ende einer im Entwurf über zwei DIN-A4 Seiten umfassenden Vorschrift.

6) Nr. 13: § 57a Anwendungen zur automatisierten Verarbeitung von an öffentlichen Orten und besonders gefährdeten öffentlichen Einrichtungen offen erhobenen personenbezogenen Daten

Die Vorschrift regelt die Befugnis zur intelligenten Videoüberwachung und biometrischen Echtzeit-Fernidentifizierung. Sie bezieht sich dabei auf § 57 Absatz 2 und 3, die die Befugnis zur Erhebung von personenbezogenen Daten durch den offenen Einsatz von technischen Mitteln zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen unter freiem Himmel, an oder in Objekten im Sinne des § 15 Absatz 1 Satz 1 Nummer 3 oder in deren unmittelbarer Nähe und an Kriminalitätsschwerpunkten, regeln. Für diese Aufnahmen soll durch § 57a künftig Künstliche Intelligenz zum Einsatz kommen können, um Bewegungsmuster, die auf die Begehung einer Straftat hindeuten, oder Muster bezogen auf Waffen, Messer und gefährliche Gegenstände automatisiert erkennen und auswerten zu können. Sofern entsprechende Muster erkannt werden und Polizeibeamt*innen der Auffassung sind, dass mit Straftaten von erheblicher Bedeutung in absehbarer Zeit mit hinreichender Wahrscheinlichkeit gerechnet werden kann, können die Einsatzkräfte eine automatisierte Nachverfolgung der verantwortlichen Personen durch die automatisierten Anwendungen veranlassen. Zusätzlich kann eine biometrische Echtzeit-Fernidentifizierung durchgeführt werden, wenn eine erhebliche gegenwärtige Gefahr für Leib oder Leben einer Person vorliegt, sofern die Abwehr dieser Gefahr auf diese Weise unbedingt erforderlich ist (Absatz 1) und sofern dies unbedingt erforderlich ist, zur Abwehr einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr durch die Begehung einer terroristischen Straftat oder zur Suche nach Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung oder vermissten Personen (Absatz 2). Für alle Maßnahmen der Echtzeit-Fernidentifizierung soll das Sächsische Staatsministerium des Innern das Nähere zum Verfahren in einer Verwaltungsvorschrift regeln (Absatz 4).

Dies lehnen wir aus den folgenden Gründen ab:

Zum einen sind wir der Auffassung, dass eine KI-basierte Videoüberwachung des öffentlichen Raums und eine daraus resultierende Echtzeit-Fernidentifizierung einen permanenten Überwachungsdruck auf die Menschen, die sich in diesem aufhalten, ausübt. Dies kann zu Verhaltensanpassungen führen, indem die entsprechenden Orte vermieden werden, Menschen vorsichtiger werden und sich nicht mehr frei bewegen können. Das stellt eine erhebliche Einschränkung aller Menschen in einer freiheitlichen Demokratie dar und es stellt sich die Frage, ob die mit der Vorschrift anvisierte Gefahrenverhinderung durch eine automatisierte Gefahrenerkennung und damit einhergehend die ggf. darauffolgende Echtzeit-Fernidentifizierung und anschließende Gefahrenbeseitigung diese Einschränkungen aufwiegt.

Daran haben wir erhebliche Zweifel.

Denn mit der Vorschrift wird in die Grundrechte einer unüberschaubaren (sich überwiegend rechtstreu verhaltenden) Anzahl von Menschen bereits durch die grundsätzliche Möglichkeit der Videoüberwachung eingegriffen, der Einsatz einer automatisierten Analyse mittels entsprechender Software verstärkt diesen Eingriff noch zusätzlich. Sollte die durch die KI durchgeführte Analyse Bewegungsmuster, die auf eine Straftat hindeuten oder Muster, die auf Waffen, Messer u.a. hindeuten, erkennen und einen entsprechenden Alarm auslösen, stellt sich die Frage, warum zur Abwehr einer davon ausgehenden erheblichen gegenwärtigen Gefahr eine Echtzeit-Fernidentifizierung geeignet sein soll, diese Gefahr abzuwenden. Wir können uns keinen Fall vorstellen, indem dies möglich sein kann. Die Abwendung der entsprechenden gegenwärtigen Gefahr wird wohl – wenn dann – nur durch einen entsprechenden Polizeieinsatz vor Ort möglich sein. Insofern ist die Möglichkeit zur Echtzeit-Fernidentifizierung nach Absatz 1 unserer Auffassung nach unverhältnismäßig und damit verfassungswidrig.

Darüber hinaus dürfte wohl keine KI auf neutralen Daten basieren. Die zugrundeliegenden Daten spiegeln vielmehr Vorurteile, Rassismus, Diskriminierung etc. wider, wodurch es zunächst zu Verzerrungen kommt, die zu falschen Verdächtigungen führen können und am Ende auch zu falschen Statistiken. Denn vorurteilsbehaftete Systeme werden entsprechend ihrer Datensätze bestimmte Menschen rausfiltern, die dann wahrnehmbar im öffentlichen Raum auch entsprechend häufiger in Maßnahmen geraten und durch häufigere Kontrollen auch häufiger Straftaten entdeckt/aufgedeckt werden. Diese Zahlen fließen am Ende in die Statistiken ein und diese wiederum befeuern polarisierende Meinungen und Strömungen und schaden so der Gesellschaft. Es ist insofern positiv zu berücksichtigen, dass die Minderheitsregierung in diesem Zusammenhang laut Begründung eigentlich keine lernenden Systeme einsetzen möchte, denn diese würden dazu führen, dass die KI auf Grundlage der oben genannten Punkte weiterlernt und diskriminierende Algorithmen vertieft. Indem in § 79c allerdings sehr umfassend und offen formuliert eine Rechtsgrundlage geschaffen werden soll, aufgrund derer sämtliche personenbezogene Daten, die der Polizei vorliegen (und damit auch die durch § 57a generierten) zum Trainieren und Testen von KI-Systemen genutzt werden können, und zwar auch durch Dritte (!), wird der in der Begründung zum Ausdruck kommende Wille, keine lernenden Systeme einzusetzen, wieder konterkariert. Gäbe es die eben beschriebene Möglichkeit durch § 79c nicht, stellt sich darüber hinaus die Frage, warum in der Gesetzesbegründung mitgeteilt wird, dass keine lernenden Systeme eingesetzt werden sollen, sich dies aber nicht im Wortlaut der Vorschrift wiederfindet. Die Gesetzesbegründung dient letztlich als Auslegungshilfe im Falle von Streitigkeiten über die Auslegung der Norm. Wäre eine klare und verbindliche Regelung zum Verbot lernender Systeme tatsächlich gewollt gewesen, wäre das in den Wortlaut der Vorschrift aufgenommen worden. Denn die Nichtaufnahme dieses Merkmals in den Wortlaut der Vorschrift und die Nennung des Willens in die Begründung spricht für eine Grundsatz-Ausnahme-Regelung.

Hinzukommt, dass uns die Möglichkeit der Kontrolle und so der Schutz der Bevölkerung vor diskriminierenden Algorithmen fehlt. Da es einige KI-Systeme gibt, die aufgrund fehlender Transparenz der dahinterstehenden Firmen und mangelnder Offenheit der zugrundeliegenden Codes nicht kontrollierbar sind und die Vorschrift keine Beschränkung der Systeme vorsieht, sondern ergebnisoffen hinsichtlich der einzusetzenden Systeme formuliert ist, fehlt die Möglichkeit, eventuell zugrundeliegende diskriminierende Algorithmen aufzudecken und zu beseitigen. Durch die offene Formulierung der Vorschrift bleibt völlig unklar, welche Systeme verwendet werden sollen. Dies öffnet Tür und Tor für private Unternehmen, die ihren Sitz ggf. im Ausland haben und dort landesrechtlichen Vorschriften unterworfen sein können, wonach sie die Daten, die sie bekommen, freigeben müssen. Darüber hinaus ist auch völlig unklar, wo welche Daten wie gespeichert werden, wie sie verarbeitet werden, was mit ihnen passiert et cetera. In der Vorschrift sind keinerlei Kontrollmöglichkeiten bzw. -verpflichtungen vorgesehen, die dies verhindern bzw. einen Einsatz entsprechend sicherer Software absichern würden.

Dies wäre auch essentiell wichtig, um eine Manipulationsanfälligkeit der Systeme so gering wie möglich zu halten. Eine KI-basierte Videoüberwachung des öffentlichen Raumes und auch die Echtzeit-Fernidentifizierung, die über die Nutzung der polizeilichen Auskunfts- und Fahndungssysteme ablaufen muss, dürften aufgrund der vielen und sensiblen, sicherheitsrelevanten Daten sehr begehrte Systeme sein, zu denen sowohl Cyberkriminelle, als auch ggf. ausländische Staaten gern Zugriff erhalten würden. Dies gilt es unbedingt zu verhindern!

Hinsichtlich der Echtzeit-Fernidentifizierung nach Absatz 2 haben wir außerdem erhebliche Zweifel an der Bestimmtheit der Norm. Denn diese enthält lediglich die Vorgabe, dass eine Echtzeit-Fernidentifizierung in den dort genannten Fällen möglich ist, wenn es unbedingt erforderlich ist. Die Maßnahme soll außerdem zeitlich und örtlich auf das unbedingt erforderliche Maß begrenzt werden. Was genau „unbedingt erforderlich“ heißt wird nicht definiert. Absatz 4 regelt zwar, dass das Sächsische Staatsministerium des Innern das Nähere zum Verfahren in einer Verwaltungsvorschrift regeln muss, dies betrifft jedoch ausweislich des Wortlauts des Absatzes 4 nicht die Verhältnismäßigkeitsabwägungen, die nach Absatz 2 getroffen werden müssen und dürfte das darüber hinaus auch gar nicht. Denn diese Abwägung ist angesichts der Intensität der Grundrechtseingriffe so wesentlich, dass die Vorgaben zur Abwägung durch den Gesetzgeber selbst geschaffen werden müssen. Dies gilt unseres Erachtens nach darüber hinaus auch für andere von der Verordnungsermächtigung in Absatz 4 erfasste Regelungsgegenstände. Gerade die Anforderungen an die Qualitätsstandards des einzusetzenden Erkennungssystems müssen in unseren Augen durch den Gesetzgeber geregelt werden. Denn mit diesen Qualitätsstandards geht einher, welche Systeme verwendet werden und wie sicher diese vor oben genannten Kritikpunkten sind. Eine Verwaltungsvorschrift entfaltet keine Außenwirkung, womit die Rechtsschutzmöglichkeiten hiergegen erheblich eingeschränkt sind. Alle wesentlichen Entscheidungen muss der Gesetzgeber deshalb selbst treffen.

Eine umfassende KI-basierte Videoüberwachung des öffentlichen Raumes und eine Echtzeit-Fernidentifizierung hat das Potenzial das Vertrauen der Menschen in staatliche Institutionen erheblich zu schwächen. Dies gilt es unbedingt zu vermeiden.

7) Nr. 16: § 62a Anlassbezogene Anwendung zur automatisierten Datenanalyse

Die Vorschrift soll eine Rechtsgrundlage zur anlassbezogenen automatisierten Zusammenführung, Verknüpfung, Aufbereitung und Auswertung von Daten bieten.

Auch diese Vorschrift lehnen wir in dieser Form sehr klar ab. Nicht, weil wir grundsätzlich die Notwendigkeit technischer Hilfsmittel für die Polizei nicht sehen, sondern weil wir durch die Verwendung automatisierter Datenanalysesysteme in der derzeitigen Fassung erhebliche Sicherheitsbedenken haben.

Hinsichtlich der grundsätzlich mit KI einhergehenden Diskriminierungsgefahr wird auf Punkt 6) verwiesen. Zwar enthält § 62a Absatz 2 im Gegensatz zum § 57a die Vorgabe, dass sicherzustellen ist, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden dürfen. Wie das sichergestellt werden soll bleibt allerdings vollkommen offen und dürfte auch technisch nur abbildbar sein, indem eine vollumfängliche und umfassende Kontrolle des verwendeten Systems möglich ist. Das Bundesverfassungsgericht hat hierzu entschieden, dass eine spezifische Herausforderung darin besteht, die Herausbildung und Verwendung diskriminierender Algorithmen zu verhindern. Daher dürften selbstlernende Systeme in der Polizeiarbeit nur unter besonderen verfahrensrechtlichen Vorkehrungen zur Anwendung kommen, die trotz der eingeschränkten Nachvollziehbarkeit ein hinreichendes Schutzniveau sichern (BVerfG 1 BvR 1547/19 Rz. 100). Diese Anforderungen sehen wir durch die Einfügung des Satzes „Bei der automatisierten Datenanalyse ist sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet, noch verwendet werden“ nicht erfüllt,

denn dieser Satz enthält keinerlei verfahrensrechtliche Vorkehrungen, die ein hinreichendes Schutzniveau sichern können. Wir sehen das hinreichende Schutzniveau auch nicht dadurch gesichert, dass die automatisierte Datenanalyse manuell ausgelöst wird und auf Grundlage von anlassbezogenen Suchbegriffen erfolgen soll, am Ende die Sachverhaltseinschätzung durch Polizeibeamt*innen getroffen wird und auch die Verarbeitungsschritte während der Datenanalyse durch den Menschen vorher festzulegen sind. Denn das sichert nicht ab, dass die der automatisierten Datenanalyse zugrundeliegenden Algorithmen nichtdiskriminierend sind. Auch Absatz 4, wonach das Sächsische Staatsministerium des Innern das Nähere zum Verfahren durch Verwaltungsvorschrift zu regeln hat, ist hierfür unseres Erachtens nicht geeignet. Darüber hinaus sind wir auch der Auffassung, dass angesichts der mit der Vorschrift einhergehenden neuen Eingriffe in das Recht auf informationelle Selbstbestimmung, wenn Daten automatisiert zusammengeführt werden, die außerdem auch intensiver sind als die Verwendung der ursprünglich erhobenen Daten, der Gesetzgeber das Nähere zum Verfahren selbst regeln muss und dies nicht auslagern darf. Hier stellen sich außerdem Anwendungsfragen, indem z.B. Absatz 3 festlegt, welche Daten zusammengeführt werden können, Absatz 4 das Sächsische Staatsministerium aber in Satz Nr. 1 ermächtigt festzulegen, welche Art der Daten zusammengeführt werden dürfen.

Im Gegensatz zu § 57a enthält § 62a nirgendwo einen Hinweis darauf, dass eine Beschränkung auf nichtlernende Systeme gewünscht bzw. vorgesehen ist (auch wenn uns eine tatsächliche Festlegung auf nichtlernende Systeme auch in § 57a fehlt und durch § 79c wieder ausgehebelt würde, s.o.). Eine Beschränkung auf nichtlernende Systeme ist verfassungsrechtlich allerdings in bestimmten Situationen sowieso zwingend geboten. Das Bundesverfassungsgericht hat dies für automatisierte Datenanalysen im Vorfeld einer konkretisierten Gefahr bereits entschieden.

Datenschutzrechtlich schließen wir uns den Ausführungen der Sächsischen Datenschutzbeauftragten an. Auch wir haben erhebliche Bedenken aufgrund des fehlenden Richtervorbehalts, fehlender Benachrichtigungspflichten, fehlender Regelungen hinsichtlich der Nutzung/Verwendung von Daten nach Abschluss der Maßnahme et cetera.

Darüber hinaus möchten wir noch einmal sehr deutlich hervorheben, dass der Einsatz der Software von Palantir Technologies für uns nicht verhandelbar ist. Palantir Technologies ist ein US-amerikanisches Unternehmen, das wirtschaftliche Interessen verfolgt und tief verbunden mit US-amerikanischen Geheimdiensten ist. Einer der ersten Geldgeber war die CIA-Tochter In-Q-Tel. Es kann deshalb nicht garantiert werden was mit Daten passiert, die diesem Unternehmen gegeben werden. Gerade wenn Sicherheitsbehörden von Palantir bereitgestellte Software nutzen, agieren diese mit hochsensiblen Daten von Bürger*innen, deren Schutz gewährleistet sein muss. Es muss sichergestellt sein, dass diese Daten nicht an andere Staaten weitergeleitet werden und/oder darüber Einfluss genommen werden kann. Auch sollte sich nicht von einem privaten, US-amerikanischen Unternehmen abhängig gemacht werden, sondern deutsche oder europäische Lösungen gesucht werden.

Hinzu kommt die Funktionsweise von Palantir. Mittels der bereitgestellten Software können Daten aus einer Vielzahl von Quellen automatisiert miteinander verknüpft werden. Es werden also riesige Datenmengen ausgewertet, Daten miteinander verknüpft und so Verbindungen hergestellt. Dies kann auch von und zu Menschen passieren, die nicht im Zusammenhang mit Straftaten stehen, sondern als Zeug*innen, Opfer oder Auskunftspersonen polizeilich geführt, im Rahmen der Datenverknüpfung mit einbezogen werden und deren Daten dann letztendlich bei einem privaten US-amerikanischen Unternehmen liegen könnten.

Schließlich ist zu beachten, dass der Programm-Code ein Geschäftsgeheimnis ist. Das bedeutet, es ist nicht nachvollziehbar wie genau Palantir Daten auswertet, verknüpft und miteinander verbindet. Dies kann dazu führen, dass Mitarbeitende von Palantir Zugriff auf die Daten bekommen, die Sicherheitsbehörden dort einspeisen und damit umfassende Einblicke in die Arbeit deutscher Sicherheitsbehörden. Darüber hinaus ist aufgrund der fehlenden

Transparenz auch nicht ausgeschlossen, dass diese Daten weitergegeben werden oder anderweitig missbraucht werden. Schließlich verhindert die Geheimhaltung des Programm-Codes jede Kontrolle von außen. Die Kontrolle dessen, was staatliche Institutionen wie Sicherheitsbehörden tun, ist jedoch essentiell in einer Demokratie und muss stets gewährleistet sein.

Aufgrund mangelnder Transparenz kann bei diesem Unternehmen außerdem nicht überprüft werden, inwiefern der Datenanalyse und -verknüpfung diskriminierende Algorithmen zugrunde liegen und so durch die Nutzung der Software bestehende Ungerechtigkeiten und Diskriminierungen nicht noch verstärkt werden. Die Schritte der Analyse, die Schritte zur Verknüpfung und die Schritte zur Verbindungsherstellung müssen im Einzelnen überprüfbar sein, damit eine Software von staatlichen Stellen eingesetzt werden kann.

Um eine für uns vertretbare Rechtsgrundlage für eine anlassbezogene Anwendung zur automatisierten Datenanalyse zu schaffen, sollte diese auf deutsche bzw. europäische Lösungen beschränkt sein, die vollumfassend transparent und kontrollierbar sind um sicherzustellen, dass diskriminierende Algorithmen weder verwendet, noch herausgebildet werden und jederzeit die volle Kontrolle zu haben, was mit den genutzten Daten genau passiert. Es braucht Richtervorbehalte, Benachrichtigungspflichten und es muss detailliert geregelt werden wie lange Daten gespeichert werden, wann sie zu löschen sind und welche Daten nicht benutzt werden dürfen. Darüber hinaus braucht es eine klare Beschränkung auf nichtlernende Systeme, die rechtmäßig austrainiert sind.

8) Nr. 16: § 62b Anlassbezogener nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

§ 62b soll eine Rechtsgrundlage für den Abgleich von zur polizeilichen Aufgabenerfüllung gespeicherten biometrischen Daten von Gesichtern und Stimmen mit öffentlich zugänglichen biometrischen Daten aus dem Internet mittels automatisierter Anwendung werden. Dies soll ausweislich der Gesetzesbegründung dem Zweck dienen, Störer*innen zu identifizieren und/oder zu lokalisieren.

Da mit diesem Abgleich die Erhebung und Verarbeitung von Daten eines nicht abgrenzbaren Personenkreises einhergeht und der Abgleich darüber hinaus wie eine heimliche Maßnahme wirkt, da er von den Betroffenen nicht bemerkt wird, stellt der Abgleich einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar.

Hinsichtlich der Nutzung automatisierter Anwendungen wird auf unsere oben bereits benannten Kritikpunkte verwiesen.

Auch hier soll das Sächsische Staatsministerium des Innern per Verwaltungsvorschrift die Anforderungen an die in den Abgleich einzubeziehenden biometrischen Daten, den technischen Verfahrensablauf und die Anforderungen an die Qualitätsstandards des einzusetzenden Erkennungssystems regeln. Angesichts der Eingriffsintensität darf auch hier der Gesetzgeber keine wesentlichen Entscheidungen auf das Sächsische Staatsministerium des Innern auslagern. Dies betrifft unserer Auffassung nach wieder die in Absatz 5 genannten Regelungsgegenstände. Welche Daten in den Datenabgleich einbezogen werden ist wesentlich für die damit einhergehenden Grundrechtseingriffe. Hinsichtlich des technischen Verfahrensablaufs sollten wenigstens die grundlegenden Linien durch den Gesetzgeber bestimmt werden, selbiges gilt für die Anforderungen an die Qualitätsstandards des einzusetzenden Erkennungssystems.

9) Nr. 18: § 64 Einsatz einer V-Person, Verdeckte Ermittlerin und Verdeckter Ermittler

Hinsichtlich der Anpassung des § 64 begrüßen wir die Ausführungen der Sächsischen Datenschutz- und Transparenzbeauftragten. § 64 Absatz 5 sollte an § 12 Absatz 2 SächsVSG angepasst werden. Es erschließt sich nicht, weshalb beim Einsatz von V-Personen durch Polizeibehörden andere Maßstäbe gelten sollen hinsichtlich der Frage wer nicht eingesetzt werden darf, als beim Einsatz von V-Leuten durch den Verfassungsschutz.

10) Nr. 19: § 66 Überwachung der Telekommunikation

§ 66 Absatz 2 und 2a enthalten Rechtsgrundlagen für die Quellen-Telekommunikationsüberwachung.

Eine Befugnis zur Überwachung und Aufzeichnung laufender Telekommunikation in der Weise, dass mit technischen Mitteln in von Betroffenen eigengenutzte IT-Systeme eingegriffen wird (Quellen-Telekommunikationsüberwachung) begründet einen sehr schwerwiegenden Eingriff sowohl in das IT-System-Grundrecht als auch in das Fernmeldegeheimnis (BVerfG NVwZ 2025, 1821). Dies scheint bei Erstellung des Referentenentwurfs nicht berücksichtigt worden zu sein. Die Gesetzesbegründung nimmt lediglich Bezug auf ein älteres Urteil des Bundesverfassungsgerichts und setzt sich darüber hinaus auch nicht mit einem Eingriff in das IT-System-Grundrecht auseinander. Auch die Begründung, mit der Quellen-Telekommunikationsüberwachung würde nur die Kommunikation erlangt, die auch durch eine konventionelle Telekommunikationsüberwachung erlangt würde, irritiert uns sehr. Wäre das der Fall, bräuchte es eine Quellen-Telekommunikationsüberwachung offensichtlich nicht. Darüber hinaus hat das Bundesverfassungsgericht bereits festgestellt, dass die Quellen-Telekommunikationsüberwachung in mehrere Grundrechte (sehr schwerwiegend) eingreift, womit es sich offensichtlich nicht lediglich um eine Telekommunikationsüberwachung in anderer Form handelt. Eine dezidierte Auseinandersetzung mit dem Thema fehlt im Referentenentwurf vollständig.

Die Quellen-Telekommunikationsüberwachung lehnen wir ab, denn diese erfolgt stets über den Einsatz entsprechender Trojanersoftware oder über eine Ausnutzung von Sicherheitslücken. Wenn Sicherheitslücken für die Quellen-TKÜ benötigt werden, dann setzt das nicht den Anreiz diese zu schließen bzw. zu melden, damit sie geschlossen werden und so Bürger*innen, deren Datensicherheit gerade akut gefährdet ist, zu schützen. Im Gegenteil – es setzt Anreize diese Sicherheitslücken offen zu halten, um sie selbst nutzen zu können. Und wenn Sicherheitslücken gekauft werden können setzt das Anreize, Sicherheitslücken zu verkaufen anstatt sie zu schließen.

Diese Sicherheitslücken nutzen aber nicht nur Sicherheitsbehörden, um an Informationen zu gelangen. Auch Cyber-Kriminelle und/oder ausländische Staaten können diese nutzen, um Systeme zu missbrauchen. Wenn staatliche Stellen von Lücken wissen, die auch Kriminelle nutzen können und diese weder schließen, noch melden, setzen sie also tendenziell alle davon betroffenen Bürger*innen einem weltweiten Missbrauchsrisiko aus. Das dürfte außer Verhältnis zum angedachten Zweck stehen „erfolgreiche Gefahrenaufklärung im Bereich von terroristischen Gefährdern oder Organisierter Kriminalität“ zu betreiben. Um dem zu entgegnen und zusätzlich der Schutzpflicht, die den Staat trifft, zu genügen, müsste der Gesetzgeber unserer Auffassung nach dafür sorgen, dass Sicherheitsbehörden verpflichtet sind, Sicherheitslücken zu melden, sobald sie sie finden. Nicht, sie weiter für sich zu nutzen.

Hinsichtlich der Veränderung technischer Systeme ist bisher nicht definiert, wie diese vorgenommen werden sollen und auch nicht, welche Veränderungen vorgenommen werden sollen. Hier muss immer mitgedacht werden, dass auch Folgeschäden entstehen können, z.B. indem eine Software durch ein vermeintlich nützliches Programm auf die Hardware gespielt

wird, die betroffene Person dieses nützliche Programm samt Schadsoftware aber so positiv bewertet, dass sie es weiter versendet und so auch bei völlig Unbeteiligten Lücken durch staatliche Institutionen provoziert werden, die dann entsprechend von Kriminellen genutzt werden können. Weder die Veränderungen, noch Vorsorgemaßnahmen um Folgeschäden zu verhindern sind im Gesetzesentwurf normiert oder irgendwo näher beschrieben. Zwar soll durch Absatz 3 sichergestellt werden, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, dass die vorgenommenen Maßnahmen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden und dass das eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung zu schützen ist. Dies zeigt jedoch zum einen sehr deutlich, dass es auch Maßnahmen gibt, die nicht (oder nicht automatisiert) rückgängig gemacht werden können und folglich die informationstechnischen Systeme auf Dauer beschädigen und angreifbar für Kriminelle machen können. Zum anderen zeigt die Vorschrift, dass nicht klar ist, was konkret für die Datenerhebung unerlässlich ist, denn das ist nirgendwo normiert.

Auch die Protokollierungsvorschriften zur Quellen-TKÜ in § 75 Absatz 1, 2 Nummer 9 werfen Fragen auf, denn es muss nur die Bezeichnung des zur Datenerhebung eingesetzten Mittels protokolliert werden. Das dürfte allerdings zu Auslegungs- und Anwendungsschwierigkeiten führen, denn was damit in Bezug auf die Durchführung einer Quellen-TKÜ gemeint ist, erschließt sich erst einmal nicht sofort. Damit könnte das informationstechnische System, in das eingegriffen wird, gemeint sein, genauso gut wie das technische Mittel, mit dem eingegriffen wird, die Software, die genutzt wird oder die Hardware, die genutzt wird oder auch all diese Punkte.

Es dürfte regelmäßig nach Beendigung einer Maßnahme nicht von Interesse der Sicherheitsbehörden sein, das technische Mittel, die Software, das System in das eingegriffen werden konnte o.ä. preiszugeben, um es weiter nutzen zu können, sodass unbestimmte Regelungen Tür und Tor öffnen, um in der Gesetzesanwendung eine sehr staatsfreundliche Auslegung zu vertreten. Dies schadet nicht nur dem Vertrauen in staatliche Institutionen, auch kommt der nachträglichen Kontrolle polizeilichen Handelns eine erhebliche Bedeutung zu und eine Protokollierung ist Grundvoraussetzung von kontrollierbaren Sachverhalten. Diese Bedeutung wächst vorliegend noch durch den manipulativen und verdeckten Charakter der auf Grundlage der Quellen-TKÜ durchgeführten Eingriffe.

Schließlich sieht die Vorschrift auch keine Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung vor, obwohl Eingriffe in diesen unzulässig und nicht zu rechtfertigen sind und die Betroffenheit angesichts der geregelten Eingriffsbefugnisse schnell denkbar und regelmäßig berührt sein dürfte.

11) Nr. 22: § 71 Einsatz von unbemannten Luftfahrtssystemen

§ 71 soll eine Rechtsgrundlage für den Einsatz von Drohnen aus Gründen der Klarstellung der Zulässigkeit der Drohnenverwendung für bestimmte Datenerhebungsmaßnahmen enthalten.

Der Einsatz von Drohnen soll recht umfassend möglich werden, im Einzelnen bei § 56 wenn es erforderlich ist zur Gefahrenabwehr, dem Schutz privater Rechte, zur Vollzugshilfe und zur Erfüllung von der Polizei durch andere Rechtsvorschriften zugewiesene Aufgaben. Allerdings nur, wenn die Offenheit der Maßnahme gewahrt bleibt und es soll auf die Verwendung von Drohnen hingewiesen werden (Absatz 1 Satz 2, 3). Der Drohneneinsatz soll außerdem zur präventiven Überwachung von fahrzeugführenden Personen im öffentlichen Verkehrsraum zur Aufdeckung der Nutzung elektronischer Geräte am Steuer (§ 23 StVO) erlaubt sein, sofern der Einsatz offen erfolgt (Absatz 1 Nummer 2), zur Observation und für den verdeckten Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen gemäß § 63 Absatz 1 und 2 (Absatz 1 Nummer 3) und zum verdeckten Einsatz technischer Mittel in oder aus Wohnungen

zum Abhören und Aufzeichnen von Bildern gemäß § 65 Absatz 1 (Absatz 1 Nummer 4). Außerdem zur Datenerhebung durch Telekommunikationsüberwachung und Quellen-Telekommunikationsüberwachung (Absatz 1 Nummer 5) und zur Datenerhebung durch den verdeckten Einsatz technischer Mittel zur Standorterhebung zum Finden hilfloser, suizidaler oder vermisster Personen gemäß § 68 Absatz 2 (Absatz 1 Nummer 6).

Hinsichtlich des § 57 Absatz 9, also der Nutzung von Drohnen um Verstöße gegen § 23 StVO aufzudecken, wurde oben bereits ausgeführt.

Hinsichtlich des Drohneneinsatzes für Datenerhebungen im Bereich der Telekommunikations- und Quellen-Telekommunikationsüberwachung erschließt sich uns nicht, warum und wie dort Drohnen zum Einsatz kommen sollen.

§ 71 Absatz 1 Satz 2 ordnet die Offenheit der Maßnahme nach Absatz 1 Nummer 1 an. Absatz 1 Satz 3 gibt den Regelfall an, dass in den Fällen der Offenheit der Maßnahme auf die Verwendung von Drohnen gesondert hingewiesen werden soll. Laut der Gesetzesbegründung kann von der Offenheit bei Gefahr im Verzug abgesehen werden. Wenn das als Ausnahmeregelung zum in Satz 3 niedergeschriebenen Regelfall angegeben worden sein sollte, steht sie im Widerspruch zu Satz 2, der keinen Regelfall, sondern eine verbindliche Anordnung der Offenheit der Maßnahme regelt. Die Gesetzesbegründung führt also entweder dazu, dass darüber die Offenheitsverpflichtung umgangen werden soll, mindestens jedoch zu Anwendungsschwierigkeiten. Hier ist dringend eine Klarstellung erforderlich, was die Minderheitsregierung genau bezwecken möchte. Angesichts dessen, dass Datenerhebungen mit Drohnen tendenziell eingriffsintensiver sein können, als die bisher bekannten stationären Datenerhebungen, sollten diese – wenn überhaupt – ausschließlich offen erfolgen dürfen. Für bestimmte Zwecke, wie die Erfassung von Verstößen gegen § 23 StVO und die Erfassung von abstrakten Gefahren nach § 57 Absatz 1 bis 3 z.B. halten wir sie für unverhältnismäßig.

12) Nr. 26: § 79b Weiterverarbeitung zu Aus- und Fortbildungszwecken, zu statistischen, archivarischen oder wissenschaftlichen Zwecken, Weiterverarbeitung von Vorgangsverwaltungs- und Protokolldaten

Absatz 2 gibt der Polizei die Befugnis, 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 weiterzuverarbeiten.

Diese Befugnis sollte schon aus Transparenzgründen nicht unter dieser Überschrift geregelt werden.

Darüber hinaus bildet Absatz 2 laut Gesetzesbegründung eine Rechtsgrundlage, die die Weiterverarbeitung von Adressdaten von Mitgliedern der extremistischen Szene ermöglicht, zu denen Erkenntnisse zur Begehung politisch motivierter Straftaten vorliegen, zum Zweck der Täteransprache und der Beratung durch die Polizei im Rahmen des Aussteigerprogramms Sachsen. Das lässt sich allerdings in der Norm mit keiner Silbe finden. Der Wortlaut der Vorschrift ist nicht ansatzweise auf die in der Begründung genannten Anwendungsfälle beschränkt, sondern so offen gefasst, dass letztendlich jede Beteiligungsform an Straftaten erfasst wird.

Hier besteht ein eklatanter Widerspruch zwischen Wortlaut und Begründung.

Darüber hinaus ist der Absatz 2 so unbestimmt gefasst, dass wir erhebliche Zweifel an der Verfassungsmäßigkeit haben. Es ist vollkommen unklar, nach welchen Kriterien sich bemessen soll, wann eine Person plant die Begehung von Straftaten durch andere Personen zu unterstützen, zu fördern, vorzubereiten oder zu planen.

13) Nr. 26: § 79c Training und Test von lernenden IT-Systemen

§ 79c soll eine Rechtsgrundlage dafür darstellen, dass die Polizei vorhandene personenbezogene Daten der Polizei zum Zweck des Trainierens und Testens von lernenden IT-Systemen weiterverarbeiten darf.

Die Frage der Datensicherheit haben wir oben bereits aufgeworfen. Diese muss sichergestellt werden, hierzu lassen sich bisher allerdings keine Anknüpfungspunkte finden.

Auch in dieser Vorschrift findet sich die Vorgabe wieder, dass sicherzustellen ist, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Auch dazu haben wir bereits ausgeführt, dass diese Absichtserklärung zwar nett ist, der Schutz vor Diskriminierung aber so essentiell, dass er rechtsverbindlich abgesichert werden muss. Wenn Systeme genutzt werden, bei denen nicht klar ist auf welchen Algorithmen sie beruhen, kann ein Diskriminierungsschutz nicht sichergestellt werden. Wir verweisen insofern auf unsere oben angeführten Kritikpunkte zum jetzigen Stand der Nutzung von Künstlicher Intelligenz.

Darüber hinaus gibt die Vorschrift vor, dass die Nachvollziehbarkeit des verwendeten Verfahrens sichergestellt sein muss, soweit dies technisch möglich ist. Dass die Nachvollziehbarkeit sichergestellt werden soll begrüßen wir ausdrücklich. Durch die Einfügung des Halbsatzes „soweit dies technisch möglich ist“ wird das Erfordernis der Nachvollziehbarkeit jedoch wieder aufgeweicht, ohne dass das notwendig wäre. Es dürfen unserer Auffassung nach schlicht nur Systeme genutzt werden, bei denen eine Nachvollziehbarkeit des verwendeten Verfahrens sichergestellt werden kann.

Dass Absatz 2 der Vorschrift ein abgestuftes System zur Anonymisierung, Pseudonymisierung und erst im letzten Schritt klaren Verarbeitung von Daten vorsieht, entspricht nicht unserer Auffassung von Datenschutz. Maßgeblich soll laut Vorschrift der „unverhältnismäßige Aufwand“ sein, der dazu führen kann, am Ende weder Anonymisierung, noch Pseudonymisierung durchsetzen zu müssen. Dieser Begriff ist auslegungsbedürftig und öffnet damit Tür und Tor um Daten einfach als Klardaten verarbeiten zu dürfen.

Gleiches gilt für Absatz 3, der die Übermittlung an Auftragsverarbeiter und Dritte regeln soll. Auch hier soll der Maßstab der „unverhältnismäßige Aufwand“ sein, was auch immer das konkret bedeuten soll.

Schließlich haben wir auch hier wieder erhebliche Zweifel am Umfang der Ermächtigung des Sächsischen Staatsministeriums des Innern in Absatz 6, per Verwaltungsvorschrift das Nähere zum Verfahren regeln zu sollen.

14) Nr. 39: § 108 Außerkrafttreten

Als Datum des Außerkrafttretens ist in der Norm der 31.12.2031 genannt, in der Begründung der 31.12.2023. Hier muss eine Klarstellung erfolgen.

Gleiches gilt im Zusammenhang mit § 40 Absatz 4 Satz 2. Diese Vorschrift soll insoweit außer Kraft treten, als dass das Sächsische Staatsministerium des Innern ermächtigt wird zu bestimmen, dass auch Polizeibeamt*innen, die außerhalb von Spezialkräften zum Einsatz kommen, der Einsatz von Vorrichtungen für den Abschluss besonderer Formen von Projektilen eröffnet wird. Laut Gesetzesbegründung soll die Regelung der Ausweitung des Einsatzes von Tasern für alle Beamt*innen befristet sein. Da aber in § 40 Absatz 4 Satz 2 das Wort Spezialkräfte gestrichen werden soll, wäre es aus Gründen der Klarheit sinnvoll, wenn die Befristung entsprechend umformuliert wird, damit allen Bürger*innen klar ist, was damit gemeint ist, wenn sie in § 40 das Wort „Spezialkräfte“ nicht mehr finden.

15) Art. 14 Inkrafttreten

Es soll das gesamte Gesetz am Tag nach der Verkündung in Kraft treten. Dies ist mit Blick auf die Vielzahl der Veränderungen, die teils erhebliche polizeipraktische sowie rechtliche und prozedurale Folgen in sich tragen, nicht nachvollziehbar.

Fazit

Abschließend möchten wir noch einmal klar und deutlich zum Ausdruck bringen, dass wir uns keineswegs versperren, die zwingend notwendigen Anpassungen des Sächsischen Polizeivollzugsdienstgesetzes durch das Urteil des Sächsischen Verfassungsgerichtshofs mit umzusetzen. Diese sind zwingend erforderlich, wenn wir nicht möchten, dass einzelne Vorschriften im Sommer 2026 außer Kraft treten. Das wäre gegenüber allen Bürger*innen und Polizeibeamt*innen im Freistaat höchst verantwortungslos. Auch eine Befugnis zur Drohnenabwehr zu schaffen erachten wir für sinnvoll und sind hier gern bereit, einer solchen Rechtsgrundlage den Weg zu bereiten.

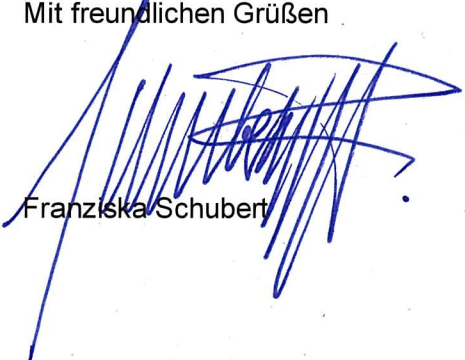
Dies nun aber zu nutzen, um eine Reihe neuer – höchst problematischer – Befugnisse zu schaffen und darauf zu vertrauen, dass diese schnell mitdiskutiert werden, weil wir unserer eigentlichen Aufgabe, bestehende Vorschriften nunmehr verfassungskonform auszugestalten, nachkommen wollen, ist unserer Auffassung nach höchst bedenklich.

Hinzu kommt, dass eine Reihe von Befugnissen geschaffen werden sollen, die den Einsatz von Künstlicher Intelligenz erlauben. Wir sind nicht grundsätzlich gegen den Einsatz von Künstlicher Intelligenz – im Gegenteil, auch wir sind der Auffassung, dass diese die Arbeit der Polizei in bestimmten Bereichen erleichtern kann. Die oben beschriebenen Risiken, wie Datensicherheit, Diskriminierung etc., müssen wir jedoch zwingend mitdenken, wenn wir solch weitreichende Befugnisse schaffen wollen! Hier erfolgt bislang keinerlei Kommunikation und auch in dem Gesetzesentwurf finden sich keinerlei Ausführungen, in welche Richtung automatisierte Anwendungen gedacht werden. Pauschale Befugnisse für deren Einsatz zu schaffen, ohne sich gleichzeitig gegen die mit gewissen Systemen und Firmen einhergehenden Risiken abzusichern, liegt uns fern. Speziell den Einsatz von Palantir lehnen wir entschieden ab. Gleiches gilt folglich für die Schaffung einer Rechtsgrundlage, die den Einsatz einer Software dieser Firma möglich machen kann.

Zusammenfassend ist der vorgelegte Gesetzentwurf aus Sicht der BÜNDNISGRÜNEN nicht zustimmungsfähig, da er in Summe einen unverhältnismäßigen Eingriff in die Freiheitsrechte der Bürgerinnen und Bürger darstellt. Die Fraktion BÜNDNIS 90/DIE GRÜNEN steht lediglich dafür bereit, bis zum 30.06.2026 ein Gesetz zu beschließen, welches die notwendigen Anpassungen an die Verfassungsrechtsprechung vornimmt und darüber hinaus eine rechtssichere Regelung für die Drohnenabwehr schafft.

Mit freundlichen Grüßen

Franziska Schubert



An die Sächsische Staatskanzlei
Herr Chef der Staatskanzlei und Staatssekretär
Dr. Handschuh
Archivstraße 1
01097 Dresden

An das Sächsische Staatsministerium des Inneren
Herrn Staatsminister Schuster
Wilhelm-Buck-Straße 2
01097 Dresden

Dresden, 04.12.2025

**Stellungnahme der BSW-Fraktion im Sächsischen Landtag
Zum Entwurf des neuen Gesetz zum PVDG**

Sehr geehrter Herr Dr. Handschuh,
Sehr geehrter Herr Schuster,

die BSW-Fraktion nimmt zum vorgelegten Entwurf wie folgt Stellung:

Stellungnahme

Die BSW-Fraktion im Sächsischen Landtag hat sich mit dem vorgelegten Entwurf eines Gesetzes zur Änderung polizeirechtlicher Vorschriften und anderer Vorschriften beschäftigt und äußert sich wie folgt:

**Artikel 1 Nummer 3
„Vorfeldstraftat“**

Die Einführung des Begriffs „Vorfeldstraftat“ im Polizeivollzugsdienstgesetz wird als rechtlich und politisch hoch umstritten eingeschätzt. Gemeint sind Handlungen, die selbst noch nicht strafbar sind, aber als Vorbereitung oder Indiz für eine spätere Straftat gewertet werden. Die

Fraktion sieht darin eine fragwürdige Vorverlagerung polizeilicher Eingriffsbefugnisse. Der Begriff ist unbestimmt und verstößt aus unserer Sicht gegen das verfassungsrechtliche Bestimmtheitsgebot. Zudem droht eine Kriminalisierung von bloßen Verdachtsmomenten oder sozial auffälligem Verhalten sowie die Verwischung der Grenze zwischen Gefahrenabwehr und Strafverfolgung. Besonders problematisch ist, dass Maßnahmen auf dieser Grundlage tief in Grundrechte eingreifen können – etwa in die Telekommunikationsfreiheit (Art. 10 GG), die Unverletzlichkeit der Wohnung (Art. 13 GG) oder die allgemeine Handlungsfreiheit (Art. 2 GG).

Das Bundesverfassungsgericht hat in vergleichbaren Fällen wie dem BKA-Gesetz oder der Vorratsdatenspeicherung bereits entschieden, dass zu weit gefasste Vorfeldbefugnisse verfassungswidrig sind. Es fordert klare Eingriffsschwellen, richterliche Kontrolle und eine enge Zweckbindung. Da die aktuelle Definition diese Anforderungen nicht erfüllt, ist eine erneute Vorlage vor dem Verfassungsgericht sehr wahrscheinlich. Aus diesem Grund lehnen wir die im Entwurf verwendete Definition ab.

Artikel 1 Nummer 10

„Einsatz von Vorrichtungen für den Abschuss besonderer Formen von Projektilen“

Die Fraktion lehnt ein flächendeckendes Roll-Out von Vorrichtungen zum Abschuss besonderer Formen von Projektilen ab. Für die sächsische Polizei außerhalb von Spezialeinheiten handelt es sich um ein neues Einsatzmittel. Ein sofortiges flächendeckendes Roll-Out würde ohne ausreichende Erfahrungswerte erfolgen und könnte zu unverhältnismäßigen Eingriffen führen. Daher ist eine stufenweise Einführung mit klarer Evaluierung zwingend erforderlich. Dafür soll die Einführung während des Erfahrungszeitraums auf ausgewählte Organisationseinheiten beschränkt werden – konkret auf ein Großstadtpolizeirevier sowie ein Revier im ländlichen Raum. So soll eine differenzierte Erprobung unter unterschiedlichen Einsatzbedingungen ermöglicht werden. Darüber hinaus fordert die Fraktion, dass bei der Anwendung dieser Vorrichtungen die Bodycam automatisch aktiviert wird. Als Voraussetzung dafür soll eine Pflicht zum Mitführen der Bodycam für die betreffenden Einsatzkräfte eingeführt werden. Auf diese Weise soll gewährleistet werden, dass der Einsatz der neuen Technik jederzeit dokumentiert und überprüfbar bleibt.

Artikel 1 Nummer 13

„Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen in Wohnungen“

Der Einsatz von Bodycam in Wohnungen wird von der Fraktion als verfassungsrechtlich sensibel eingestuft. Zwar wird die Notwendigkeit einer Befugnisenerweiterung gesehen und die im Gesetz vorgesehenen Schutzbestimmungen zum Einklang mit dem Grundrecht auf Unverletzlichkeit der Wohnung gewürdigt, zugleich wird aber auf die besondere Tragweite dieser neuen Befugnis hingewiesen. Daher fordert die Fraktion eine Befristung der Befugnisenerweiterung bis zum 31.12.2029, sowie eine umfassende Evaluierung der praktischen Anwendung und der Auswirkungen der Vorschrift nach diesem Erfahrungszeitraum von drei Jahren, spätestens bis zum 31. Dezember 2029. Die Staatsregierung soll sodann dem Landtag Bericht erstatten und der SLT erneut über die Befugnisse entscheiden. Zudem soll die Befugnisnorm durch eine Klarstellung ergänzt werden, wonach der Einsatz von Bodycam nicht mit einer allgemeinen Überwachung von Wohnungen verbunden sein darf – in Anlehnung an die Regelung im Bayerischen Polizeiaufgabengesetz.

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

Die im § 57a vorgesehene Möglichkeit einer biometrischen Echtzeit-Fernidentifizierung von Personen wird von der Fraktion als besonders schwerwiegender Eingriff in die Grundrechte bewertet. Sie berührt unmittelbar das Recht auf informationelle Selbstbestimmung und eröffnet die Gefahr einer faktischen Massenüberwachung im öffentlichen Raum. Da die Norm keine hinreichend klare Eingriffsschwelle erkennen lässt und damit unverhältnismäßig erscheint, lehnt die Fraktion diese Befugnis ab. Zugleich erkennt sie die Notwendigkeit und Sinnhaftigkeit der übrigen Regelungen im § 57a an und teilt diese.

„Anlassbezogene automatisierte Kennzeichenerkennung“

Die Fraktion bewertet die Regelung in § 58 Absatz 1 Nummer 5, wonach die automatisierte Kennzeichenerkennung dann zulässig sein soll, „wenn Tatsachen die Annahme rechtfertigen, dass dort (...) Straftaten von erheblicher Bedeutung begangen werden sollen“, als zu extensiv, da der Normzweck die Nähe zur Grenze ist. Es bleibt unklar, welche Delikte konkret erfasst werden sollen. Zudem stellt sich die Frage, warum diese Befugnis ausschließlich im Grenzgebiet gelten soll und nicht darüber hinaus. Vor diesem Hintergrund vertritt die Fraktion die Auffassung, dass der Einsatz der automatisierten Kennzeichenerkennung im Grenzgebiet ausschließlich auf die Verhinderung von Straftaten mit unmittelbarem Grenzbezug beschränkt werden muss. Damit soll eine klare Eingrenzung der Befugnis erreicht und eine unverhältnismäßige Ausweitung verhindert werden.

Artikel 1 Nummer 26

„Training und Test von lernenden Systemen“

Die Fraktion sieht die in § 79c vorgesehene Möglichkeit, zum Training und Test von lernenden IT-Systemen auch nicht anonymisierte personenbezogene Daten zu verwenden, kritisch. Gefordert wird stattdessen, dass ausschließlich anonymisierte personenbezogene Daten eingesetzt werden dürfen, um den Schutz der Privatsphäre und das Recht auf informationelle Selbstbestimmung zu gewährleisten.

Darüber hinaus hält die Fraktion eine Evaluierungspflicht für erforderlich, in dem die Erforderlichkeit, die praktische Anwendung und die Auswirkungen der Maßnahmen nach einem Erfahrungszeitraum von drei Jahren, spätestens jedoch bis zum 31. Dezember 2029, durch die Staatsregierung überprüft werden. Dabei hat die oder der Sächsische Datenschutz- und Transparenzbeauftragte Stellung zu nehmen. Über die Ergebnisse der Evaluierung sowie die Stellungnahme ist dem Landtag zu berichten.

Damit stellt die Fraktion klar, dass aus ihrer Sicht technologische Innovationen zwar unterstützt werden, diese aber nur unter strengen Datenschutzauflagen und mit klarer parlamentarischer Kontrolle zulässig sein sollen.

Artikel 1 Nummer 28

„Öffentlichkeitsfahndung“

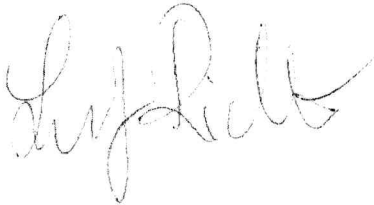
Die im Entwurf verwendete Formulierung erlaubt eine Öffentlichkeitsfahndung bereits dann, wenn von einer Person eine „Gefahr“ für Leib, Leben oder Freiheit anderer Personen ausgeht. Nach allgemeiner polizeirechtlicher Definition liegt eine Gefahr vor, wenn bei ungehindertem Ablauf des Geschehens mit hinreichender Wahrscheinlichkeit ein Schaden für ein polizeiliches Schutzgut eintreten wird. Diese Schwelle ist vergleichsweise niedrig und umfasst auch Situationen, in denen ein Schaden lediglich möglich erscheint.

Demgegenüber bezeichnet die „dringende Gefahr“ eine qualifizierte Gefahrenlage. Sie liegt vor, wenn ein Schaden für besonders wichtige Rechtsgüter – wie Leib, Leben oder Freiheit – unmittelbar bevorsteht oder wenn die Wahrscheinlichkeit des Schadenseintritts besonders hoch ist. Damit ist die Eingriffsschwelle deutlich enger gefasst und auf gravierende Situationen beschränkt.

Eine Öffentlichkeitsfahndung stellt einen besonders intensiven Eingriff in die Grundrechte der betroffenen Person dar, insbesondere in das allgemeine Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung. Sie führt zu einer breiten öffentlichen Stigmatisierung und kann erhebliche soziale Folgen nach sich ziehen. Daher ist es verfassungsrechtlich geboten, die Befugnis nur bei einer dringenden Gefahr zuzulassen.

Die Änderung stellt sicher, dass Öffentlichkeitsfahndungen nicht bei bloßen Verdachtsmomenten oder abstrakten Gefahrenlagen erfolgen, sondern ausschließlich in Situationen, in denen ein schwerer Schaden für Leib, Leben oder Freiheit anderer Personen unmittelbar droht. Damit wird der Grundrechtsschutz gestärkt und zugleich die Verhältnismäßigkeit der Maßnahme gewahrt.

Mit freundlichen Grüßen

A handwritten signature in black ink, appearing to read 'Lutz Richter', written in a cursive style.

Lutz Richter (MdL)
Parlamentarischer Geschäftsführer

DER VORSITZENDE

CDU-Fraktion des Sächsischen Landtages
Bernhard-von-Lindenau-Platz 1 | 01067 Dresden

Chef der Staatskanzlei und Staatssekretär
für Bundes- und Europaangelegenheiten
Herrn Dr. Andreas Handschuh
Sächsische Staatskanzlei
Archivstraße 1
01097 Dresden

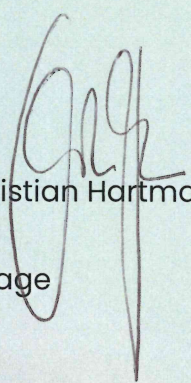
Dresden, 9. Dezember 2025

Stellungnahme der CDU-Fraktion zum PDVG

Sehr geehrter Herr Staatssekretär,

bezugnehmend auf Ihr Schreiben vom 2. Oktober 2025 an Herrn Landtagspräsidenten Alexander Dierks, MdL, übersende ich Ihnen die Stellungnahme der CDU-Fraktion des Sächsischen Landtags zum Entwurf des Gesetzes zur Änderung polizeirechtlicher Vorschriften und anderer Vorschriften.

Mit freundlichen Grüßen



Christian Hartmann, MdL

Anlage

Stellungnahme der CDU-Fraktion im Sächsischen Landtag

zum Entwurf eines Gesetzes zur Änderung polizeirechtlicher Vorschriften

Teil A – Grundsätzliche Stellungnahme

Die CDU-Fraktion im Sächsischen Landtag begrüßt den vorliegenden Entwurf eines Gesetzes zur Änderung polizeirechtlicher Vorschriften ausdrücklich. Der Entwurf setzt die Vorgaben des Sächsischen Verfassungsgerichtshofs (Urteil vom 25. Januar 2024, Vf. 91-II-19) sowie die einschlägige Rechtsprechung des Bundesverfassungsgerichts um und stärkt zugleich die Handlungsfähigkeit des sächsischen Polizeivollzugsdienstes. Er schafft die dringend erforderliche Rechtsklarheit und Rechtssicherheit für die sächsische Polizei und trägt damit maßgeblich zur Gewährleistung der inneren Sicherheit im Freistaat bei.

Seit der letzten grundlegenden Reform des Polizeirechts im Jahr 2019 haben sich die Rahmenbedingungen der polizeilichen Arbeit erheblich verändert. Die fortschreitende Digitalisierung, neue technische Tatmittel, hybride Bedrohungslagen und die stetig wachsende Informationsdichte stellen die Polizei vor neue, komplexe Herausforderungen. Gleichzeitig ist die Erwartung der Bürgerinnen und Bürger an eine wirksame Gefahrenabwehr und Kriminalitätsbekämpfung unverändert hoch. Die CDU-Fraktion teilt daher ausdrücklich die Einschätzung des Staatsministeriums des Innern, dass diese Anforderungen nur durch eine Anpassung der polizeilichen Eingriffsbefugnisse an die tatsächlichen Gefährdungslagen erfüllt werden können.

- Aus Sicht der CDU-Fraktion greift der Gesetzentwurf die maßgeblichen höchstrichterlichen Leitentscheidungen auf, stärkt Kontrollmechanismen, wahrt den Grundsatz der Verhältnismäßigkeit und erweitert zugleich sachgerecht und maßvoll die Handlungsmöglichkeiten der Polizei dort, wo dies aus fachlicher Sicht unabdingbar ist. Dies gilt insbesondere für folgende Regelungen: Mit der **Einführung der anlassbezogenen automatisierten Datenanalyse (§ 62a SächsPVDG)** wird die Polizei in die Lage versetzt, vorhandene Datenbestände mit Hilfe moderner Technologien effektiv auszuwerten. Diese Regelung ist angesichts der fortschreitenden Digitalisierung und der Komplexität polizeilicher Lagedarstellungen aus Sicht der CDU-Fraktion unerlässlich, denn sie schafft eine Rechtsgrundlage für den Einsatz bestehender Systeme und die künftige Integration lernender Softwarelösungen, ohne den Charakter der Maßnahme als anlassbezogen und kontrolliert zu verändern.
- Die CDU-Fraktion im Sächsischen Landtag befürwortet entschieden die Einführung des § 62b SächsPVDG zum **anlassbezogenen nachträglichen biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet**. Diese Regelung schafft erstmals eine rechtssichere Grundlage, um in besonders gefährlichen Lagen gezielt biometrische Daten wie Gesichts- oder Stimmprofile mit öffentlich verfügbaren Datenquellen abzugleichen. Sie ist damit eine notwendige Antwort auf die digitale Realität moderner Gefahrenlagen, in der sich Täter zunehmend in sozialen Netzwerken, Videoplattformen und Onlineforen bewegen.

§ 62b SächsPVDG reagiert damit auf ein reales Vollzugsdefizit. Bislang war ein gezielter Abgleich solcher Daten rechtlich kaum möglich, obwohl die Technik seit Jahren existiert und im Ausland erfolgreich genutzt wird – etwa bei Fahndung nach untergetauchten Straftätern.

- Die **Regelung zur „intelligenten Videoüberwachung“ (§ 57a SächsPVDG)** stellt ein modernes und verhältnismäßiges Instrument zur frühzeitigen Gefahrenabwehr dar. Sie ermöglicht eine gestufte, EU-datenschutzkonforme Analyse von Bilddaten zur Erkennung sicherheitsrelevanter Muster, zur Nachverfolgung von Störern und im Einzelfall zur Echtzeitidentifizierung. Damit wird die Polizei in die Lage versetzt, u. a. an kriminalitätsbelasteten Orten präventiv und lageangepasst zu handeln.
- Die CDU-Fraktion spricht sich für die ausdrückliche gesetzliche Zulassung des **verdeckten Einsatzes der automatisierten Kennzeichenerfassung (AKES) (§ 58 SächsPVDG)** aus. Während der offene Betrieb von Kennzeichenerfassungssystemen vor allem der Verkehrsüberwachung und der allgemeinen Fahndung dient, eröffnet der verdeckte Einsatz aus Sicht der Fraktion eine zusätzliche Möglichkeit zur wirksamen Bekämpfung mobiler und grenzüberschreitender Kriminalität. Diese Einschätzung wird von der Überzeugung getragen, dass verdeckte AKES-Systeme insbesondere im Rahmen mobiler Kontrollen, bei internationalen Fahndungslagen und im grenznahen Raum einen wichtigen Beitrag zur Identifizierung von Tätergruppen und zur Aufklärung krimineller Bewegungsmuster leisten können. Die CDU-Fraktion befürwortet daher eine gesetzliche Regelung des verdeckten Einsatzes, sofern dieser auf konkrete Lageerfordernisse beschränkt bleibt und mit Nichttrefferlöschung und Protokollierungspflichten verbunden ist. Für die CDU-Fraktion ist klar: Eine solche Regelung würde Rechtssicherheit schaffen, den zielgerichteten Einsatz bestehende Systeme ermöglichen und die polizeiliche Bekämpfung organisierter Kriminalität wirksam stärken.
- Die CDU-Fraktion unterstützt weiterhin mit Nachdruck die Einführung der **Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) als Instrument der Gefahrenabwehr**. Sie ist unverzichtbar, um in verschlüsselten Kommunikationsumgebungen handlungsfähig zu bleiben. Angesichts der zunehmenden Nutzung verschlüsselter Kommunikationsdienste durch Tätergruppen stoßen Sicherheitsbehörden im Bereich der Gefahrenabwehr mit herkömmlichen Mitteln zunehmend an ihre Grenzen, da die konventionelle Telekommunikationsüberwachung nur Kommunikationsdaten im Übertragungsnetz erfassen, nicht aber die Inhalte verschlüsselter Messenger-Dienste wie WhatsApp, Signal, Telegram oder Threema. Ohne die Befugnis zur Quellen-TKÜ und der damit verbundenen Ermöglichung zum Auslesen kryptierter Kommunikation bliebe es auch weiterhin unmöglich, bestimmte wesentliche Erkenntnisse zur Verhinderung schwerwiegender Straftaten, etwa im Bereich des Terrorismus oder der Organisierten Kriminalität, zu gewinnen. Wir begrüßen es daher ausdrücklich, dass diese Befugnis mit dem vorliegenden Gesetzesentwurf geschaffen wird.

- Angesichts des starken Einsatzes unbemannter Fluggeräte in den vergangenen Jahren und Monaten ist die **Schaffung von Befugnissen zur Drohnenabwehr (§ 12a SächsPVDG)** für die CDU-Fraktion unabdingbar. Ohne eine ausdrückliche gesetzliche Befugnis zur Erkennung, Überwachung und Abwehr solcher Systeme besteht für die Polizei keine rechtssichere Grundlage, um diese Gefahren zu unterbinden. Die in § 12a SächsPVDG vorgesehene Regelung schafft hier Klarheit und Handlungssicherheit. Sie erlaubt es, gefährdende oder unerlaubte Drohnenflüge zu lokalisieren, deren Steuerung zu unterbrechen und, wenn erforderlich, technische Maßnahmen zur Abwehr zu ergreifen. Die Maßnahme ist auf konkrete Gefahrenlagen beschränkt, unterliegt der Verhältnismäßigkeitsprüfung und dient dem unmittelbaren Schutz von Leib, Leben und kritischer Infrastruktur.
- Die CDU-Fraktion spricht sich entschieden für **die Erweiterung des Bodycam-Einsatzes auf Wohnungen** aus (**§ 57 Abs. 4 SächsPVDG**), da Polizeibedienstete insbesondere bei Einsätzen in Wohnungen besonderen Gefährdungen ausgesetzt sind. Gerade in Fällen häuslicher Gewalt, bei psychischen Ausnahmelagen oder Bedrohungen im familiären Umfeld sind Beamtinnen und Beamte häufig massiven Aggressionen ausgesetzt. Die Regelung trägt damit insbesondere auch der Notwendigkeit Rechnung, den Schutzauftrag für unsere Polizeibeamten entsprechend ernst zu nehmen: Der Einsatz der Bodycam wirkt nachweislich deeskalierend und gewaltpräventiv. Der vorgesehene Regelungsentwurf beschränkt die Anwendung von Bodycams in Wohnungen auf das Vorliegen konkreter gesteigerter Gefahrenlagen und wahrt den Schutz des Kernbereichs privater Lebensgestaltung.
- Die Erweiterung polizeilicher **Befugnisse zur Bekämpfung häuslicher Gewalt und „Stalking“ (§§ 19, 61, 84 SächsPVDG)** führt aus Sicht der CDU-Fraktion zu einer erheblichen Verbesserung des Opferschutzes. Von zentraler Bedeutung ist dabei insbesondere auch die Herabsetzung der Eingriffsschwelle, um es den Beamten zu ermöglichen, schneller und damit zielgerichteter zu agieren. Mit der Neuordnung der Befugnisse wird zugleich die Handlungssicherheit der Polizei gestärkt und ihnen ein klarer Maßnahmenkatalog an die Hand gegeben.

Die CDU-Fraktion im Sächsischen Landtag unterstützt den Gesetzentwurf daher vollumfänglich. Eine Abschwächung oder Einschränkung einzelner Befugnisse würde die Wirksamkeit der Normen erheblich mindern und dem praktischen Sicherheitsbedürfnis im Freistaat Sachsen zuwiderlaufen.

Teil B – Bewertung ausgewählter Regelungen gemäß Anhörungsschreiben

Im Folgenden wird der im Anhörungsschreiben formulierten Bitte nachgekommen, neben einer grundsätzlichen fachlichen Bewertung des Gesetzentwurfs insbesondere zu einzelnen, im Entwurf besonders hervorgehobenen Regelungsbereichen Stellung zu nehmen

1. Verwendung des Begriffs der „Vorfeldstraftat“ (§ 4 Nummer 6 SächsPVDG)

Durch die Aufnahme des Begriffs der Vorfeldstraftat in die Begriffsbestimmungen sowie seine ergänzende Nennung in den §§ 21, 60, 61, 63, 64, 66, 67 und 68 werden die von der Rechtsprechung des Sächsischen Verfassungsgerichtshofs geforderten Einschränkungen der Eingriffsschwellen rechtssystematisch nachvollziehbar umgesetzt.

Die Begriffsbestimmung in § 4 Nummer 6 erfasst sowohl Straftaten, die strafbare Vorbereitungshandlungen darstellen, als auch solche, die lediglich eine Gefährdung von Rechtsgütern beinhalten. Damit umfasst sie alle Straftaten, bei denen keine konkrete Gefahr für das geschützte Rechtsgut erforderlich ist. Durch die vorgesehene Regelungssystematik wird anknüpfend an den Begriff der Vorfeldstraftat normiert, dass bestimmte eingriffsintensive Befugnisregelungen zur Verhütung von Straftaten, die bloße Vorbereitungshandlungen oder Rechtsgütergefährdungen unter Strafe stellen, nur dann zur Anwendung gelangen dürfen, wenn zumindest tatsächliche Anhaltspunkte für eine Gefahr für das jeweilige geschützte Rechtsgut vorliegen.

2. Erweiterung des Rechtsguts der „öffentlichen Ordnung“ (§ 18 SächsPVDG)

Die CDU-Fraktion hält die Wiederaufnahme des Schutzguts der „öffentlichen Ordnung“ in § 18 SächsPVDG für dringlich geboten. Mit der Beschränkung der Erteilung von Platzverweisen auf die Abwehr von Gefahren für das Rechtsgut der „öffentlichen Sicherheit“ werden bestimmte Störerlagen, wie beispielsweise aggressives Betteln, koordiniertes Blockaden- oder Einschüchterungsverhalten mit dem Ziel der Störung genehmigter Veranstaltungen oder extreme Ruhestörungen nicht erfasst. Auch solches Störerverhalten beeinträchtigt das friedliche Zusammenleben aber erheblich. Vor diesem Hintergrund befürwortete die CDU-Fraktion die Wiederaufnahme der Regelung im „alten Polizeigesetz“, das die Möglichkeit zur Platzverweisung zur Abwehr von Gefahren für die „öffentliche Ordnung“ beinhaltete. Mit der neuerlichen Ergänzung der Vorschrift würde das redaktionelle Versehen der Streichung des Begriffs im Rahmen der letzten Novelle in der Vorschrift des § 18 korrigiert.

Vor diesem Hintergrund stößt eine Wiederaufnahme auf ausdrückliche Unterstützung der CDU-Fraktion, da so die notwendige Handlungssicherheit der Polizei gestärkt und zugleich an den bundesweit bestehenden Regelungsstandard angeknüpft wird.

3. Bewertung der Regelung des § 57a SächsPVDG (automatisierte Datenverarbeitung an öffentlichen Orten)

Die in § 57a vorgesehene Befugnis zur automatisierten Verarbeitung offen erhobener personenbezogener Daten ist ein zentraler Bestandteil moderner Gefahrenabwehr und wird

von der CDU-Fraktion daher ausdrücklich begrüßt. Ohne die in § 57a SächsPVDG vorgesehene Regelung wäre es künftig ausgeschlossen, der zunehmenden Dynamik sicherheitsrelevanter Ereignisse im öffentlichen Raum frühzeitig adäquat begegnen zu können.

Mit § 57a wird eine gestufte und streng zweckgebundene Befugnis zur automatisierten Auswertung offen erhobener Bilddaten geschaffen. Nach Auffassung der CDU-Fraktion trägt die Regelung dem Umstand Rechnung, dass akute Bedrohungssituationen – insbesondere in unübersichtlichen Lagen oder bei großen Menschenansammlungen – durch ausschließlich manuelle Beobachtung nur eingeschränkt erfasst und bewertet werden können. Die Erfahrung – auch aus anderen Bundesländern – zeigt, dass der Einsatz automatisierter Verfahren in diesen Fällen eine frühzeitige Erkennung auffälliger Muster ermöglicht, etwa dem Mitführen von gefährlichen Gegenständen oder aggressivem Verhalten. Es ist daher aus Sicht der CDU-Fraktion unzweifelhaft, dass die Regelung der Polizei in solchen Fällen wertvolle Zeitvorteile für ein rechtzeitiges und verhältnismäßiges Eingreifen verschafft. Die mehrstufige Ausgestaltung stellt sicher, dass der Eingriffsumfang jeweils an den Grad der tatsächlichen Gefahr angepasst bleibt. Zugleich gewährleisten die vorgesehenen Kontrollmechanismen – wie die verpflichtende menschliche Überprüfung, der Richtervorbehalt, die Unterrichtung der Sächsischen Datenschutz- und Transparenzbeauftragten bei abgeschlossenen Maßnahmen der Stufe 3 bzw. bei Maßnahmen nach Abs. 2 sowie weitere umfassende Dokumentations- und Berichtspflichten – eine rechtsstaatlich ausgewogene Anwendung. Auf Grundlage dieser Einschätzung hält die CDU-Fraktion die Einführung der Regelung für einen notwendigen und zielführenden Schritt, mit dem die polizeiliche Gefahrenabwehr um ein zeitgemäßes Instrument ergänzt wird, das die Effizienz polizeilichen Handelns verbessert, ohne den Grundrechtsschutz der Betroffenen zu vernachlässigen.

Die CDU-Fraktion im Sächsischen Landtag unterstützt zudem die in § 57a Absatz 2 SächsPVDG vorgesehene Befugnis zur **gezielten Fern-Identifikation**: Die Fraktion erkennt die Befugnis als notwendige Ergänzung der polizeilichen Möglichkeiten zur Gefahrenabwehr, die eine bestehende Lücke zwischen der offenen Videoüberwachung (§ 57) und der nachträglichen Datenanalyse (§ 62a) schließen dürfte.

Aus Sicht der CDU-Fraktion ist es mit Blick auf die dynamischen Gefahrenlagen, mit denen die Polizei zunehmend konfrontiert ist, unabdingbar, ihr den Einsatz gezielter Fern-Identifikation zu ermöglichen. So wird die Polizei in die Lage versetzt, in einer konkreten Gefahrensituation oder im Rahmen der Fahndung nach gefährlichen Personen biometrische Merkmale, die im Rahmen der Videoüberwachung offen erhoben wurden, gezielt mit polizeilichen Fahndungsbeständen abzugleichen.

Die CDU-Fraktion sieht hierin eine Befugnis von erheblicher praktischer Bedeutung: In polizeilichen Lagen mit vielen Beteiligten – etwa bei Großveranstaltungen, Demonstrationen, Fußballspielen oder Anschlagslagen – ist es mit herkömmlichen Mitteln kaum möglich, Verdächtige in Echtzeit zu identifizieren, ohne die Sicherheit der Einsatzkräfte oder Unbeteiligter zu gefährden. Die gezielte Fern-Identifikation wird entsprechend als Möglichkeit gesehen, eine konkrete Zielperson in laufenden

Videostreamen zu erkennen und zu lokalisieren, um unmittelbar geeignete Maßnahmen zur Gefahrenabwehr einleiten zu können.

Da sich die Maßnahme ausdrücklich nicht auf eine flächendeckende oder anlasslose Gesichtserkennung richtet, sondern auf gezielte, verfahrensgebundene Einzelfälle, und weiterhin die Voraussetzung einer erheblichen gegenwärtigen Gefahr für Leib oder Leben gegeben sein muss, wird die Befugnis aus Sicht der CDU-Fraktion den Anforderungen an rechtsstaatliche Kontrolle und die Wahrung bürgerrechtlicher Anliegen gerecht. Die Befugnis darf nur angewendet werden, wenn sie unbedingt erforderlich ist. Damit bleibt der Eingriff auf Ausnahmesituationen begrenzt, in denen ein sofortiges Handeln notwendig ist, um Menschen vor schweren Gewalttaten zu schützen.

Folgerichtig bewertet die CDU-Fraktion § 57a als unverzichtbaren Baustein eines modernen Polizeigesetzes. Der Einsatz lernender Systeme und KI-gestützter Auswertung zu den genannten Zielen ist europarechtlich und verfassungsrechtlich zulässig und erscheint polizeifachlich dringend erforderlich.

4. Drittbetroffenheit in § 66 Abs. 2a Nr. 4 und 5 SächsPVDG (Telekommunikationsüberwachung)

Die CDU-Fraktion hält ausdrücklich an dem Erfordernis einer Regelung zur Zulässigkeit der Quellen-Telekommunikationsüberwachung auch bei Nachrichtennutzern (Personen, die Mitteilungen für die betroffene Person weitergeben oder entgegennehmen) oder Dritten (Personen, die ihr Handy dem Störer zur Nutzung überlassen) fest. Gerade bei der Gefahrenaufklärung im Bereich organisierter Kriminalität oder terroristischer Straftaten nutzen betroffene Personen Kommunikationsmittel Dritter oder Dritte, um die Gefahr einer Eigenüberwachung zu umgehen. Die Streichung dieser Regelung würde die praktische Bedeutung der Befugnisregelung erheblich minimieren. Die CDU-Fraktion vertritt in diesem Zusammenhang die Auffassung, dass für die Gefahrenabwehr dringend erforderlich ist, ggf. auch auf die Kommunikation von Dritten oder Nachrichtennutzern zugreifen zu können. Durch die vorgesehenen Eingriffsschwelle, dass aufgrund bestimmter Tatsachen angenommen werden kann, dass der Nachrichtennutzer oder der Dritte eng in den Kommunikationsaustausch eingebunden ist, ist aus Sicht der CDU-Fraktion sichergestellt, dass Verdachtsgründe über vage Hinweise hinausgehen müssen. Durch die verfahrensrechtliche Anforderung des Richtervorbehalts wird die Anforderungen an eine solche Maßnahme vollumfänglich abgesichert.

Die CDU-Fraktion hält die Norm für ausgewogen und sachgerecht. Aus Sicht der Fraktion ermöglicht sie wirksame Gefahrenabwehr in komplexen Kommunikationsstrukturen, ohne den Schutz Unbeteiligter zu vernachlässigen.

Teil C – Über den Entwurf hinausgehende weiterführende Bedarfe

Die CDU-Fraktion im Sächsischen Landtag begrüßt den Gesetzentwurf in seiner Gesamtausrichtung ausdrücklich. Zugleich zeigen die aktuellen sicherheits- und gesellschaftspolitischen Entwicklungen, dass bestimmte Befugnisse und Regelungen, die in anderen Ländern bereits erfolgreich umgesetzt werden, auch im Freistaat Sachsen rechtlich

verankert werden sollten. Ziel muss es sein, den Polizeivollzugsdienst bestmöglich auszustatten, um auf moderne Bedrohungsformen, technische Entwicklungen und komplexe Einsatzlagen wirksam reagieren zu können.

1. Erweiterung des § 57 SächsPVDG – Videoschutz an „gemiedenen Orten“

Die CDU-Fraktion spricht sich für die Einführung einer Befugnis zur offenen Videoüberwachung an sogenannten „gemiedenen Orten“ aus. Hierbei handelt es im Verständnis der CDU-Fraktion, angelehnt an das hessische Polizeigesetz, um Bereiche des öffentlichen Raums – etwa Unterführungen, Parkanlagen, Bahnsteige oder schlecht beleuchtete Durchgänge –, die aufgrund einzelner Delikte oder Gefährdungslagen von der Bevölkerung gemieden werden und als sogenannte „Angsträume“ gelten.

Es ist ein zentrales Anliegen der CDU-Fraktion, sowohl die objektive Sicherheit als auch das subjektive Sicherheitsgefühl der Bürgerinnen und Bürger zu stärken und Unsicherheitsempfindungen ernst zu nehmen. Erfahrungen aus anderen Bundesländern - insbesondere Hessen und Nordrhein-Westfalen - zeigen, dass offen gekennzeichnete Videoüberwachung an kriminalitätsbelasteten oder sicherheitsrelevanten Orten zu einer deutlichen Reduzierung von Straftaten und zu einer höheren Aufklärungsquote führen. Vor diesem Hintergrund misst die CDU-Fraktion einer Erweiterung von Videoschutzmaßnahmen auf „gemiedene Orte“ besondere Bedeutung bei.

Die Maßnahme erscheint verhältnismäßig, da sie auf konkret bezeichnete Orte, auf klare Lagebewertungen und auf enge Zweckbindungen begrenzt werden kann. Durch Lösch- und Protokollierungspflichten wäre auch ein wirksamer Datenschutz gewährleistet.

Die CDU-Fraktion hält eine solche Regelung für geboten, um die Handlungsfähigkeit der Polizei im Bereich der präventiven Gefahrenabwehr zu stärken und den Schutz potenzieller Opfer zu verbessern. Sie spricht sich daher für die Ergänzung des § 57 um eine Befugnis zur offenen Videoüberwachung an gemiedenen Orten aus.

2. Erweiterung der Regelung zur Verkehrsüberwachung (§ 57 Abs. 9 SächsPVDG)

Aus Sicht der CDU greift die in § 57 Abs. 9 implementierte Reduzierung der Verkehrsüberwachung auf die unerlaubte Nutzung elektronischer Geräte (= Handys) zu kurz und wird dem Ziel, besonders sicherheitsrelevante Verkehrsordnungswidrigkeiten zu verhüten, nicht gerecht. Zu präferieren wäre daher eine Erweiterung der Regelung auf Regelverstöße wie ungenügenden Sicherheitsabstand oder auch Vorfahrtsverstöße. Handlungsleitend muss aus Sicht der CDU-Fraktion hier die „Vision Zero“ sein. Zudem erscheint die Anknüpfung der Kontrolle von Handyverstößen nach § 23 Abs. 1a StVO an bestimmte Streckenabschnitte nicht praxisgeeignet, da entsprechende Verstöße regelmäßig im gesamten öffentlichen Verkehrsraum begangen werden und eben nicht räumlich oder zeitlich konzentriert an bestimmten Streckenabschnitten.

3. Einführung einer Befugnis zur Online-Durchsuchung (§ 69a SächsPVDG)

Die CDU-Fraktion hält die Schaffung einer landesrechtlichen Befugnis zur Online-Durchsuchung für zwingend erforderlich: Der Polizeivollzugsdienst muss in die Lage

versetzt werden, mit den technologischen Entwicklungen und den zunehmend hochprofessionellen Methoden moderner Kriminalität Schritt zu halten. Kriminelle Strukturen – insbesondere im Bereich der organisierten Kriminalität, des Extremismus und Terrorismus sowie der sexualisierten Gewalt gegen Kinder – verlagern ihre Kommunikation und Datenspeicherung zunehmend in verschlüsselte digitale Räume.

Der CDU-Fraktion erscheint es vor diesem Hintergrund unabdingbar, es der Polizei mittels der Befugnis zur Online-Durchsuchung zu ermöglichen, auf gespeicherte, verschlüsselte Daten in IT-Systemen oder Cloud-Umgebungen zuzugreifen, wenn dies zur Abwehr einer Gefahr u. a. für höchstrangige Rechtsgüter wie Leben, Gesundheit oder Sicherheit und Bestand der öffentlichen Sicherheit unerlässlich ist. Ohne eine entsprechende Befugnis droht der Polizei nach Einschätzung der CDU-Fraktion ein erheblicher Verlust operativer Handlungsfähigkeit im digitalen Raum.

Gerade in Verfahren wegen des Besitzes und der Verbreitung von kinderpornografischen Inhalten, bei Cybergrooming oder im Bereich extremistischer Netzwerke zeigt sich für die CDU-Fraktion deutlich die Notwendigkeit dieser Befugnis. Erfahrungsgemäß nutzen Täter verschlüsselte Kommunikationswege, geschlossene Foren und Anonymisierungsdienste, um Beweise zu verbergen oder zu vernichten. Der Zugriff auf gespeicherte abgeschlossene Kommunikationsinhalte kann hier entscheidend sein, um Täterstrukturen aufzudecken, Missbrauchstaten zu verhindern oder Anschläge zu vereiteln. Die CDU-Fraktion bewertet die Online-Durchsuchung daher als unverzichtbares Instrument einer zeitgemäßen und modernen Gefahrenabwehr, das den rechtssicheren Zugriff auf digitale Beweismittel ermöglicht und zugleich dem hohen Schutzniveau des Grundrechtsrahmens Rechnung trägt.

4. Präzisierung im Rahmen des § 62a SächsPVDG – Einsatz von KI-gestützten Datenanalyseverfahren

Die CDU-Fraktion begrüßt die im Gesetzentwurf enthaltene Einführung der anlassbezogenen automatisierten Datenanalyse (§ 62a SächsPVDG) und spricht sich ausdrücklich für eine Zulassung auch KI-gestützter Verfahren aus.

Die CDU-Fraktion sieht, dass die polizeiliche Arbeit zunehmend von großen, heterogenen Datenmengen geprägt ist, deren gezielte Auswertung mit „menschlichen Mitteln“ schon allein aufgrund der schieren Menge an auszuwertenden Daten mitunter unmöglich ist. Moderne Auswertungssysteme, die Muster, Netzwerke oder dynamische Entwicklungen erkennen können, stellen aus Sicht der CDU-Fraktion daher eine notwendige Voraussetzung für eine effektive und zeitgerechte Gefahrenabwehr dar. KI-basierte Verfahren bieten die Möglichkeit, Daten aus unterschiedlichen Quellen effizient zusammenzuführen und zu analysieren, wobei selbstverständlich insbesondere die Kriterien menschlicher Kontrolle, eine klare Zweckbindung und dokumentierte Nachvollziehbarkeit gewährleistet sein müssen.

Fraktion Die Linke im Sächsischen Landtag
Bernhard-von-Lindenau-Platz 1, 01067 Dresden

Sächsische Staatskanzlei
Chef der Staatskanzlei
Dr. Andreas Handschuh
Archivstraße 1
01097 Dresden

**Fraktion Die Linke
im Sächsischen Landtag**

SUSANNE SCHAPER
Fraktionsvorsitzende

LUISE NEUHAUS-WARTENBERG
Parlamentarische
Geschäftsführerin

Bernhard-von-Lindenau-Platz 1
01067 Dresden

Telefon: 0351 493-5800
linksfraktion@slt.sachsen.de
www.linksfraktion-sachsen.de

Ostsächsische Sparkasse
Dresden
DE50 8505 0300 3120 2007 26
OSDDDE81XXX

Dresden, 10. Dezember 2025

Stellungnahme gemäß Nummer I Ziffer 3 SächsKIV

der Fraktion Die Linke im Sächsischen Landtag

zum Referentenentwurf mit dem Titel:

„Gesetz zur Änderung polizeirechtlicher Vorschriften“

I. Gesetzesanliegen

Der vorliegende Referentenentwurf für ein Gesetz zur Änderung polizeirechtlicher Vorschriften dient insbesondere der Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG). Bei den vorgesehenen zahlreichen Änderungen handelt es sich zum einen um redaktionelle Klarstellungen sowie um zwingende Anpassungen an die geänderte Rechtslage und die zwischenzeitlich ergangene verfassungsgerichtliche Rechtsprechung, primär des Sächsischen Verfassungsgerichtshofs und sekundär des Bundesverfassungsgerichts. Zum anderen handelt es sich um fakultative, wahlweise rechts- und kriminalpolitisch oder polizeifachlich begründete Änderungen und Erweiterungen bestehender sowie um die Aufnahme neuer eingriffsintensiver Befugnisse.

Besonders hervorzuheben sind dabei die vorgesehenen Regelungen zur Drohnenabwehr und zum Einsatz von Drohnen zur präventiven Verkehrsüberwachung, zur Ausweitung des Einsatzes von Bodycams auf Wohnungen, zur Quellen-TKÜ, zur Ausgestaltung der automatisierten Kennzeichenerkennung als verdeckte Maßnahme, zur Möglichkeit der Freigabe des Einsatzes des sogenannten Tasers als Waffe über den bisher auf Spezialeinheiten beschränkten Gebrauch hinaus, zu verschiedenen Maßnahmen zum Schutz vor häuslicher Gewalt und Nachstellungen, darunter der erweiterte Einsatz der elektronischen Fußfessel und die Möglichkeit der Datenweitergabe an Beratungsstellen sowie schließlich eine ganze Reihe von Befugnissen im Hinblick auf – teils hochriskante – KI-Anwendungen, wie die intelligente Videoüberwachung durch Verhaltensmustererkennung, Personennachverfolgung und biometrische Echtzeitidentifizierung, eine Analyseplattform, die retrograde biometrische Onlineidentifizierung sowie das Training von KI-Systemen anhand polizeilicher Echtdaten.

II. Vorbemerkungen zur Bewertung des Gesetzgebungsvorhabens

Der Umfang des Gesetzgebungsvorhabens bedingt eine differenzierte Betrachtung. Anhand der im Abschnitt III. folgenden Einzelbewertung zu einer Auswahl der seitens der Fraktion die Linke als maßgeblich befundenen Regelungen werden sich aus hiesiger Sicht zur Beseitigung bestehender Bedenken konkrete Änderungen am Referentenentwurf teils zwingend erforderlich ma-

chen. Den regelungsspezifischen Betrachtungen sind zunächst einige regelungsübergreifende Bemerkungen unter Anzeige änderungsbedürftiger Aspekte voranzustellen.

1. Umsetzung der Maßgaben aus dem Urteil des Sächsischen Verfassungsgerichtshofs vom 25. Januar 2024

Eine Reihe von Neuregelungen sind unmittelbare Folge des Urteils des Sächsischen Verfassungsgerichtshofs vom 25. Januar 2024 (Vf. 91-II-19), worin konkrete gesetzliche Bestimmungen des SächsPVDG und des Sächsischen Polizeibehördengesetzes (SächsPBG) für teilweise unvereinbar mit der Verfassung des Freistaates Sachsen erklärt wurden. Nach den hierbei vom Verfassungsgerichtshof getroffenen Feststellungen sind bei bestimmten eingriffsintensiven polizeirechtlichen Befugnisregelungen die Eingriffsschwellen durch den Verweis auf Straftatenkataloge zu niedrigschwellig gefasst, so dass schon bloße Vorbereitungshandlungen oder Rechtsgütergefährdungen genügen, damit die Polizei von diesen Befugnissen Gebrauch machen kann. Verfassungsrechtlich gefordert ist hingegen, dass im jeweiligen Einzelfall zumindest auch tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen müssen.

Es ist aus Sicht der Fraktion Die Linke zu rügen, dass das Urteil erst jetzt in ein Änderungsvorhaben überführt wird, obwohl dies wesentlich früher möglich gewesen wäre und auch dementsprechend mit einer parlamentarischen Initiative frühzeitig eingefordert wurde (vgl. den Antrag in Drucksache 8/713); und dass die Umsetzung des Urteils nun zugleich mit einer erheblichen Zahl weiterer Änderungen verbunden wird, die mit dem o. g. Urteil des SächsVerfGH in keinerlei Zusammenhang stehen und die ihrerseits einer ausführlichen Erörterung im parlamentarischen Verfahren bedürfen. Da sich jedoch aus dem Urteil ergibt, dass die erfolgreich angefochtenen Befugnisse seither nur unter vom Gericht bestimmten Maßgaben längstens bis zum Ablauf des 30. Juni 2026 anwendbar sind, tritt durch den vonseiten der Staatsregierung verursachten Verzug ein erheblicher Zeitdruck zum Abschluss des gesamten Gesetzgebungsvorhabens ein. Mithin führt diese von der Staatsregierung – noch dazu bei einem Gesetzesvorhaben, mit dem erhebliche Eingriffe in die verfassungsrechtlich garantierten Grund- und Freiheitsrechte zugelassen werden sollen – allein zu verantwortende Verfahrensweise zu einer rechtlich nicht unbedenklichen zeitlichen Restringierung der Freiheit der Willensbildung und damit der Parlamentsautonomie, was vermeidbar gewesen wäre.

- a) Dies vorangestellt, genügt der Referentenentwurf den verfassungsgerichtlichen Anforderungen überwiegend:

Durch eine Änderung der Begriffsbestimmungen in § 4 erfolgt zunächst klarstellend und ergänzend zu den weiteren befugnispezifischen Änderungen mit der neuen Nr. 6 die Legaldefinition von „Vorfeldstraftat“. Inwieweit diese – für polizeigesetzliche Regelungen neue und wohl einmalige – Legaldefinition in der Rechtsanwendung praktikabel und geeignet sein wird, den diesbezüglichen Anforderungen des SächsVerfGH zur Vermeidung von Grundrechtseingriffen bei bloßen Vorbereitungshandlungen oder Rechtsgütergefährdungen zu genügen, muss sich im Zuge der Anhörung von Sachkundigen im Gesetzgebungsverfahren erst noch erweisen.

Darüber hinaus geändert wird in Nr. 5 die (bestehende) Legaldefinition „terroristische Straftat“ nach den verfassungsgerichtlichen Anforderungen auch des BVerfG dahingehend, dass grundrechtsintensive Eingriffsbefugnisse nur dem Schutz besonders gewichtiger Rechtsgüter (Leib, Leben, Freiheit der Person, Bestand oder Sicherheit des Bundes oder eines Landes) zu dienen haben; insoweit erfolgt eine Beschränkung auf die in § 129a Abs. 1 und 2 Nr. 2 bis 5 StGB genannten Straftaten.

Spezifische Änderungen zu Bestandsbefugnisse wurden sodann dahingehend vorgenommen, dass das Aufenthaltsverbot und -gebot mit dem geänderten § 21 Abs. 2 Nr. 1 und 2 sowie das Kontaktverbot mit dem geänderten § 21 Abs. 2 Satz 3, die Ausschreibung von Personen im Fall einer terroristischen Straftat mit dem geänderten § 60 Abs. 1 Satz 1 Nr. 2, die elektronische Aufenthaltsüberwachung („elektronische Fußfessel“) im Fall einer terroristischen Straftat mit dem geänderten § 61 Abs. 1 Satz 1 Nr. 3, die Datenverarbeitung, eingeschlossen die Erstellung eines Bewegungsbildes, in Fällen terroristischer Straftaten sowie im Hinblick auf Straftatbestände, die eine Gefahr für Leib, Leben, Freiheit oder die sexuelle Selbstbestimmung begründen (Hochrisiko-Fälle von häuslicher Gewalt und Nachstellung) mit dem neuen § 61 Abs. 2 Satz 8 sowie schließlich die längerfristige Observation im Fall einer Straftat von erheblicher Bedeutung oder einer terroristischen Straftat mit dem geänderten § 63 Abs. 2 Satz 1 Nr. 2 oder 3 jeweils bei Vorfeldstraftaten dahingehend eingeschränkt sind, dass eine entsprechende Maßnahme nur zulässig ist, wenn tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen.

Zudem gilt für den Einsatz von Vertrauenspersonen (VP) und Verdeckten Ermittlern (VE) per Verweis in § 64 Abs. 1 auf die insoweit ergänzte o. g. Regelung zur längerfristigen Observation diese Vorgabe unmittelbar. Bei der Telekommunikationsüberwachung (TKÜ) im Fall einer Straftat im Sinne des § 100a Abs. 2 StPO in Bezug auf bestimmte Rechtsgüter erfolgt in § 66 Abs. 1 Nr. 2 eine Ergänzung, dass „im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für ein solches Rechtsgut vorliegen“ müssen. Für die Erhebung von Verkehrs- und Nutzungsdaten sowie für die Identifizierung und Lokalisierung von Mobilfunkgeräten gilt per Verweis in § 67 Abs. 1 bzw. § 68 Abs. 1 auf die insoweit ergänzte vorgenannte Regelung zur TKÜ die dortige Vorgabe unmittelbar. Keine gesonderte Änderung erfolgt zwar bei den Benachrichtigungspflichten nach § 74 mit der Möglichkeit, vom Einsatz einer VP oder eines VE betroffene Person nicht zu benachrichtigen, auch wenn deren Einsatz nur wegen Vorbereitungshandlungen erfolgt war. Dem vom SächsVerfGH in der Nichtbenachrichtigung erkannte Verstoß gegen das Übermaßverbot dürfte aber mit der Änderung in § 64 Abs. 1 Satz 1 i. V. m. § 63 Abs. 2 Satz 2 abgeholfen sein, wonach der VP/VE-Einsatz von vornherein nur zulässig ist, wenn im Einzelfall tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen.

Darüber hinaus wurden die Anforderungen des SächsVerfGH an die Weiternutzung bevorrateter Daten (Polizeiliches Auskunftssystem) nach dem bisherigen § 80 Abs. 2, der nicht normenklar und daher nicht verfassungsgemäß ist, umgesetzt und die Maßgabe zur Anwendung des § 79 Abs. 2 bis 5 in das neue Regelungskonzept zur sog. vorsorgenden Speicherung in den §§ 80, 80a, 80b, 80c durch Verweise auf die Weiterverarbeitungsbefugnis im neuen § 79a Abs. 2 überführt.

- b) Der Referentenentwurf genügt den verfassungsgerichtlichen Anforderungen in Bezug auf § 30 SächsPBG, betreffend die gemeindliche Videoüberwachung, jedoch nicht:

Nach dem Urteil des SächsVerfGH mangelt es § 30 Abs. 1 Nr. 2 SächsPBG an Bestimmtheit und Normenklarheit, auch soweit nicht ersichtlich ist, welche öffentliche Anlagen oder Einrichtungen erfasst werden. Mit der vorgeschlagenen Neuregelung wird die Bezeichnung dieser Örtlichkeiten („öffentliche[r] Anlagen oder Einrichtungen“) zwar ersetzt durch die Formulierung „an, in oder in unmittelbarer Nähe von öffentlichen Einrichtungen, öffentlichen Verkehrs-

mitteln, Kulturgütern, Dienstgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen“. Jedoch ist die längere Enumeration nicht wesentlich bestimmter. Vielmehr wird die Bestimmtheit der Örtlichkeit zusätzlich dadurch reduziert, dass nun auch die „unmittelbare Nähe“ der nach wie vor unbestimmten Örtlichkeiten mitumfasst sein soll. Dies ist zu ändern.

- c) Der Referentenentwurf genügt den verfassungsgerichtlichen Anforderungen auch dahingehend überwiegend, dass sie bei weiteren Änderungen, darunter auch neue Befugnisnormen, Berücksichtigung finden:

Die nähere Bewertung dieser Befugnisse zunächst dahingestellt, werden die biometrische Echtzeit-Fernidentifizierung im Fall einer terroristischen Straftat nach dem neuen § 57 Abs. 2 Satz 1 Nr. 1 sowie die biometrische retrograde Online-Identifizierung im Fall einer Straftat gem. § 100a Abs. 2 StPO oder einer terroristischen Straftat nach dem neuen § 62b Abs. 1 Satz 2 unter den Vorbehalt gestellt, dass die Maßnahme bei einer Vorfeldstraftat nur zulässig ist, wenn im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen. Für die Quellen-TKÜ und für die Unterbrechung oder Verhinderung der Telekommunikation gelten mit dem neuen § 66 Abs. 2 und mit dem geänderten § 66a (bisher: § 69) die dementsprechenden Vorgaben zur TKÜ. Darüber hinaus ergibt sich die Erforderlichkeit, mit dem neuen § 62a eine bereichsspezifische Befugnis zur automatisierten Datenanalyse („Analyseplattform“) zu schaffen, aus der Beurteilung der bestehenden allgemeinen Datenverarbeitungsbefugnis in § 80 Abs. 1 durch den SächsVerfGH dahingehend, dass diese nicht zu automatisierten Datenanalysen oder -auswertungen ermächtigt.

- d) Der Referentenentwurf genügt den verfassungsgerichtlichen Anforderungen mit den neuen § 57 Abs. 9 SächsPVDG, betreffend Bildübertragung und -aufzeichnung zur Verhütung einer besonders sicherheitsrelevanten Verkehrsordnungswidrigkeit, jedoch nicht:

Nach der Entscheidung des SächsVerfGH müssen Eingriffsschwellen für Datenerhebungsbefugnisse an tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut anknüpfen. Daran fehlt es vorliegend aber von vornherein. Durch die Befugnisnorm verfolgt werden sollen stattdessen abstrakte Gefährdungsdelikte unterhalb Strafbarkeitsschwelle, mithin gänzlich frei von der Voraussetzung des Vorliegens einer

konkreten Gefahr für irgendein bestimmtes Rechtsgut. Dieser Verfassungsverstoß ist nur zu ändern durch Streichung der Norm.

2. Befugnisse zur Nutzung „Künstlicher Intelligenz“ (KI)

Es steht aus Sicht der Fraktion Die Linke außer Frage, dass bestimmte Regelungsziele mit der Hilfe von KI-Anwendungen verfolgt und diese zur effizienten Bewältigung bestehender polizeilicher Aufgaben im Rahmen gesetzlicher Zwecke unter Wahrung datenschutzrechtlicher Vorgaben eingesetzt werden könnten. Auf dem Stand der Technik vorstellbar ist ein breites Spektrum an Softwareassistenzen für regelmäßige Ermittlungstätigkeiten zu konkreten Lebenssachverhalten, beispielsweise für eine weitgehend maschinelle Audiotranskription und die strukturierte inhaltliche Aufbereitung von TKÜ-Aufzeichnungen, als Unterstützung zur automatisierten Auswertung von Asservaten sowie zur Sichtung und Bewertung etwa von Missbrauchsdarstellungen sowie zur Analyse von Massendaten im Hinblick auf die Isolation von Datenmustern, etwa für das Auffinden von Kreuztreffern in Funkzellenabfragen.

Solche Instrumente sieht der Referentenentwurf aber nicht vor. Konzipiert werden stattdessen vier gesonderte Befugnisnormen für die „intelligente Videoüberwachung“ unter Einsatz einer Bildanalysesoftware zur Mustererkennung, zur automatisierten Personennachverfolgung und zur Echtzeit-Fernidentifizierung (§ 57a), für die automatisierte Datenanalyse auf einer KI-gestützten „Analyseplattform“ (§ 62a), für den retrograden biometrischen Identitätsabgleich mit Internetdaten (§ 62b) und für das Training von KI-Systemen anhand polizeilicher Datenbestände (§ 79c). Während diese einzelnen Befugnisnormen auch in sich höchst unterschiedlich strukturiert sind, berühren sie, ihre nähere Bewertung zunächst dahingestellt, ihrer Natur nach und aufgrund der konkreten Umsetzung einige gemeinsame Grundprobleme.

- a) Es ist nicht hinreichend klar und daher eindeutig klarzustellen, um welche Art von KI-System(en) es sich handeln soll, die im Rahmen dieser neuen Befugnisse genutzt werden dürfen:

Dem Normentext nach erfolgt nur zu § 79c eine Festlegung dahingehend, dass es sich um ein selbstlernendes KI-System handeln werde. In der Begründung wird der Zweck des Trainierens und Testens sodann auf alle weiteren KI-Befugnisse in §§ 57a, 62a, 62b bezogen. Zugleich heißt es dort in Bezug auf alle diese KI-Befugnisse, dass das Ziel darin bestehe, „nachvollziehbare Datenverarbeitungsschritte in der jeweiligen [...] Software unveränderlich zu

programmieren und damit die jeweilige spezifische Datenverarbeitung [...] durch austrainierte und ausgelernte Systeme zu ermöglichen“ (S. 99). Desgleichen bestimmen die jeweiligen Normen aber in sämtlichen Fällen nicht. Lediglich in der Begründung zu § 57a heißt es, es werde sich dort um ein „aus-trainiertes und ausgelerntes System“ handeln (S. 70). Zu § 62a ergibt sich, dass dort ein „selbstlernendes System“ zu Grunde liegen soll (S. 84), was der Begründung zu § 79c offensichtlich widerspricht. Zu § 62b findet sich eine Festlegung weder im Normtext, noch in der Begründung.

Diese Ausprägung von Technologieoffenheit ist im vorliegenden Zusammen-
hang ein untauglicher Ansatz aufgrund der prinzipiellen, nicht nur technolo-
gisch relevanten Unterschieden zwischen selbstadaptiven („lernenden“) und
deterministischen (bzw. „ausgelernten“) Systemen. Es hängen daran auch Un-
terschiede für die verfassungsrechtlichen Anforderungen, für die Einschät-
zung der Konformität mit der KI-VO und z. B. für die Gewährleistung der im
Entwurf selbst enthaltenen Bestimmung, „dass diskriminierende Algorithmen
weder herausgebildet noch verwendet werden“ – so in § 62a Abs. 2 Satz 2,
jedoch ohne jegliche Erwägungen dazu, wie die Herausbildung solcher Algo-
rithmen im Fall der in der Begründung angenommenen Verwendung eines
selbstlernenden Systems überhaupt verhindert werden könnte. Die an sich
begrüßenswerte Zielstellung nachvollziehbarer, d. h. auch in ihrer Rechtmä-
ßigkeit nachprüfbarer Datenverarbeitungsschritte ist mit selbstlernenden
Systemen im operativen Einsatz nicht zu erreichen. Es ist daher sowie aus
Gründen der Normenklarheit und Bestimmtheit zwingend erforderlich, im
Normtext selbst festzulegen, dass es sich bei §§ 57a, 62a, 62b jeweils nicht
um selbstlernende KI-Systeme handeln darf.

b) Der Normtext trifft keine hinreichenden Bestimmungen zu wesentlichen
Verfahrensfragen, sondern verlagert sie in untergesetzliche Vorschriften:

Der Referentenentwurf sieht mit § 57a Abs. 4 Satz 3 zur biometrischen Echt-
zeit-Fernidentifizierung, mit § 62a Abs. 4 Satz 1 zur automatisierten Daten-
analyse auf der KI-gestützten Analyseplattform, mit § 62b Abs. 5 zum ret-
rograden biometrischen Identitätsabgleich mit Internetdaten sowie mit § 79c
Abs. 6 zum KI-Training anhand polizeilicher Datenbestände jeweils vor, das
Nähere zum Verfahren in (später) zu erlassenden Verwaltungsvorschriften zu
regeln. Zu § 79c wird dabei nicht einmal bestimmt, dass diese VwV zu veröf-
fentlichen ist.

Es ist zunächst darauf hinzuweisen, dass sich schon aus dem Rahmen, den das Bundesverfassungsgericht zur automatisierten Datenanalyse in seinem Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 – vorgegeben hat, unmittelbar ergibt, dass Verfahren, Methoden sowie auch Beschränkungen von Abgleichsmöglichkeiten im Gesetz selbst geregelt sein müssen. Dies erwartet die Fraktion Die Linke auch im vorliegenden Fall und im Hinblick auf die wesentlichen Verfahrensfragen in Bezug auf sämtliche für das SächsPVDG vorgesehenen KI-Normen. Denn ungeachtet der Tatsache, dass die Klärung grundsätzlicher Fragestellungen ohnehin nicht grundlos – der Referentenentwurf führt keine Gründe an – in dem Gesetzgebungsverfahren nachgelagerte und damit dem Parlament entzogene untergesetzliche Regelungen verschoben werden sollten, muss es dem Parlament ganz besonders im vorliegenden Fall angesichts der Tragweite seiner gesetzgeberischen Entscheidung über eingriffsintensive Befugnisnormen durch präzise Darlegungen im Normentext selbst ermöglicht werden, sie in ihren konkreten Anwendungen und Auswirkungen tatsächlich und rechtlich einzuschätzen – u. a. auch im Hinblick auf die mangels weiterer Angaben zum Verfahren aktuell nicht näher nachprüf-bare Konformität mit der KI-VO. Der Gesetzgeber muss wissen, was er beschließt; dem entspricht es nicht, den Entwurf ausgerechnet an rechtlich wie politisch sensiblen Stellen auf eine „Blankettnorm“ zur Verweisung der betreffenden Regelung auf die unterhalb von Gesetzen und Rechtsverordnungen liegende Ebene von (rein exekutiven) Verwaltungsvorschriften zu reduzieren.

- c) Für die Umsetzung von KI-Systemen dürfen nur uneingeschränkt zuverlässige und vertrauenswürdige Anbieter in Betracht gezogen werden:

Die sinnvolle Eingrenzung in Frage kommender Softwareanbieter sowie von Dritt- oder Auftragsverarbeitern – egal ob im Rahmen landeseigener oder landesübergreifender KI-System-Lösungen – ist nicht nur nach technischen (und haushälterischen) Gesichtspunkten vorzunehmen, sondern auch nach den Erwägungsgründen der KI-VO sowie insbesondere unter dem Gesichtspunkt der Gewährleistung digitaler Souveränität. Dem trägt der Referentenentwurf bisher nicht hinreichend Rechnung. Ein zustimmungsfähiger Entwurf muss es aus Sicht der Fraktion Die Linke von vornherein sicher- und im Normentext selbst auch für die Zukunft unmissverständlich klarstellen, dass ausschließlich Produkte uneingeschränkt zuverlässiger und vertrauenswürdiger Anbieter in die Auswahl einbezogen und eingesetzt werden. Nicht uneingeschränkt vertrauenswürdig sind die Produkte extremistischer Oligarchen außerhalb bundes-deutscher und europäischer Jurisdiktion.

Die Fraktion Die Linke unterstellt nicht, dass das SMI beabsichtigt, die Auswahl für geeignet befundener Software auf einen bestimmten großen Anbieter (z. B. „Palantir“) zulaufen zu lassen. Eine solche Auswahl wäre auf der Grundlage der derzeit vorliegenden Regelungen aber ebenso wenig ausgeschlossen. Zwar erklärt die Begründung des Referentenentwurfs die Auswahl und überdies auch die Frage für gänzlich offen, ob entsprechende Produkte eigenentwickelt werden, externe Dienstleister in Anspruch genommen oder mehrfach für vorzugswürdig erklärten Bundeslösungen beigetreten werden kann. Indes werden zu § 79c bereits Vorkehrungen für die Inanspruchnahme (irgend-)eines Dritt- oder Auftragsverarbeiters getroffen, ohne weitere Positivkriterien oder negative Ausschlussgründe anzusetzen. Dies kann sich als folgenreich erweisen, da die einzelnen KI-Befugnisse für den Fall der Auswahl eines Drittanbieters auch nicht unabhängig voneinander zu betrachten sind. Denn soweit das KI-Training gemäß § 79c darauf abzielt, austrainierte und ausgelernte Systeme zur Nutzung im Rahmen der weiteren KI-Befugnisse zur Verfügung zu stellen (S. 99), entsteht eine technische Abhängigkeit der getrennten Befugnisnormen durch das Erfordernis der Kompatibilität der entwickelten bzw. genutzten Modelle. Dies dürfte die Auswahl eines einzigen, „großen“ Anbieters begünstigen.

Der vorgeblichen Unentschiedenheit bei der Auswahl von Anbieter und Software entspricht es im Übrigen nicht, dass bei der anlassbezogenen Anwendung zur automatisierten Datenanalyse nach § 62a einer unbekannten Software bereits bestimmte Funktionalitäten zugeschrieben und voraussichtliche Kosten im Rahmen der Bereitstellung in einem länderübergreifenden Verfahren beziffert werden. Darüber hinaus erfolgen zur retrograden biometrische Onlineidentifizierung nach § 62b sogar bereits Erwägungen über absehbare Kostensteigerungen und das Vertriebsmodell („monatliche Lizenzen für eine flexibel kündbare Anwendung“) einer unbenannt bleibenden Software für den Fall, dass es nicht zu einem länderübergreifenden Verfahren kommt (S. 58).

- d) Die vorgesehenen Berichtspflichten zu den KI-Befugnissen genügen nicht, empfohlen wird eine inhaltlich erweiterte Berichtsform:

Mit § 107 SächsPVDG bestehen die jährlichen (öffentlichen) Berichtspflichten gegenüber dem Landtag über abgeschlossene Maßnahmen fort und werden im Hinblick auf neue Befugnisse u. a. erweitert auf die KI-Befugnisse in § 57a Abs. 1 Satz 4 und Abs. 2 zur biometrischen Echtzeit-Fernidentifizierung, in

§ 62a zur automatisierten Datenanalyse auf der KI-gestützten Analyseplattform sowie in § 62b zum retrograden biometrischen Identitätsabgleich mit Internetdaten. Dies findet die Zustimmung der Fraktion Die Linke. Sie regt darüber hinaus an, in diesen Fällen zur Herstellung von Transparenz und zur Steigerung der Akzeptanz sich für eine erweiterte, inhaltlich über abstrakt-statistische Angaben hinausgehende Berichtsform zu entscheiden, bei der nach Vorbild der Berichtspflicht zur Transparenzplattform in § 17 Abs. 2 Satz 2 SächsTranspG regelmäßig über die Umsetzung und Anwendung, eingeschlossen die vorangehenden und begleitenden technisch-organisatorischen Maßnahmen, informiert wird. Ein solcher Bericht sollte insbesondere auch über technisch-organisatorischen Maßnahmen im Hinblick auf KI-Training anhand polizeilicher Datenbestände nach § 79c berichten.

III. Vorgesehene Gesetzesänderungen und Bewertung im Einzelnen

Im aktuellen Entwurfsstand begegnet das Gesetzgebungsvorhaben aus Sicht der Fraktion Die Linke teils keinen weiteren Bedenken. Es ist zugleich, wie vorstehend bereits angerissen, zu einem anderen, nicht unerheblichen Teil und damit aktuell insgesamt nicht zustimmungsfähig. Im Einzelnen werden ausgewählte Regelungen wie folgt bewertet:

Zu § 12a (Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme)

Neu eingeführt wird eine spezifische Befugnis zur Drohnenabwehr, gerichtet auf bzw. gegen unbemannte Fahrzeugsysteme an Land, in der Luft oder zu Wasser. Es dürfen demnach technische Mittel zur Erkennung der Gefahr und zu deren Abwehr gegen das System, dessen Steuerungseinheit und -verbindung eingesetzt werden.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, der aktuelle Entwurfsstand bedarf jedoch Änderungen. Der Regelung vorauszusetzen ist die Sicherstellung der Gesetzgebungskompetenz der Länder für die Drohnenabwehr. Im Hinblick auf die Drohnenabwehr im Rahmen des SächsPVDG ist festzuhalten, dass das praktizierte Verfahren aus dem Normentext nicht deduzierbar ist und unter Verweis auf Geheimschutzbelange auch auf Nachfrage seit je im Vagen gehalten wird (vgl. zuletzt die Kleine Anfrage in Drucksache

8/4188). Mag dies im Hinblick auf die Wahrung der Effektivität des Abwehrsystems nachvollziehbar sein, vermag die Fraktion Die Linke schwerlich einem Verfahren zuzustimmen, das sie nicht ansatzweise überblickt.

Ausgehend von der Begründung wird tatsächlich eine Vielzahl von Methoden in Betracht gezogen, nämlich „Laser, Jamming, GPS-Störung [...] sowie [...] physische Mittel“ (S. 63). Darüber hinaus muss im Mindesten erkennbar werden, ob das Abwehrverfahren lediglich darauf ausgeht, die kontrollierte Landung eines Unbemannten Luftfahrtsystems (ULS) z. B. durch Auslösung einer Notfall- bzw. „Return to home“-Funktion oder das Hijacking der Steuerung zu forcieren, oder aber auch die offensive Destruktion („Abschuss“) mit der möglichen Folge des unkontrollierten Niedergangs samt nicht auszuschließenden Schadensfolgen für Leib und Leben umfasst. Ist dieser zweite Fall der Absturzprovokation nicht ausgeschlossen, begründen Polizeimaßnahmen gegen fliegende Drohne eine Gefährdung der Allgemeinheit und erfordert der Einsatz der Drohnenabwehr nicht-triviale (Rechtsgüter-)Folgeabwägungen, die nicht in das rein situative Belieben einzelner – dann ggf. auch einzeln haftender – Polizeivollzugsbeamtinnen und -beamten, sondern unter den Vorbehalt einer fallweisen Anordnung oder jedenfalls einer einsatzbezogenen Freigabe durch die Präsidentin oder den Präsidenten des Landeskriminalamtes oder einer Polizeidirektion gestellt werden sollten. In Bezug auf die Aufzählung des Lasers als anwendbares „technisches Mittel“ ist anzumerken, dass es sich durch die damit bezweckte Einwirkung auf Sachen nicht bloß um ein technisches Mittel handelt. Da die Einordnung als Hilfsmittel körperlicher Gewalt abwegig erscheint, liegt vielmehr die Einordnung als Waffe nahe. Die insoweit unveränderte, abschließende Aufzählung in § 40 Abs. 4 Satz 1 SächsPVDG enthält den Laser jedoch ebenso wenig wie die nicht weiter aufgeschlüsselten „physischen Mittel“, falls es sich dabei nicht um Schusswaffen handeln soll.

Zu der in der Begründung aufgeführten Möglichkeit der Inanspruchnahme von Mittelzuweisungen des Bundes (S. 56) ergeht vorsorglich der Hinweis, dass bei der Auswahl, Beschaffung und Finanzierung entsprechender Systeme für die Polizei die Staatsregierung gehalten ist, die grundgesetzliche Trennung von Polizei und Militär nicht dadurch zu unterlaufen, indem sie für den polizeilichen Gebrauch militärische Systeme beschafft oder für die Beschaffung Mittel aufwendet, die gem. § 87a Abs. 1a GG dem Zweck der Stärkung der Verteidigungsfähigkeit dienen, worin kein polizeilicher Zweck liegt.

Zu § 15 (Identitätsfeststellung, hier: Kontrolle in Fahrzeugen)

Mit der Einfügung des neuen Abs.1 Satz 1 Nr. 5 wird die Identitätsfeststellung bei Personen in einem zur gezielten Kontrolle ausgeschriebenen Fahrzeug ermöglicht, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme zur Abwehr einer Gefahr erforderlich ist.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, dem Entwurfsstand begegnen keine Bedenken. Dies gilt auch in Bezug auf die weiteren Änderungen in Abs. 1 Satz 1 Nr. 6 und 7 (bisher Nr. 5 und 6) betreffend Kontrollstellen und Kontrollbereiche mit Anpassungen an das zwischenzeitlich novellierte Sächsische Versammlungsgesetz (SächsVersG) sowie an das SächsPBG. Anders, als in der Begründung angenommen wird, handelt es sich bei der Kontrolle in Fahrzeugen allerdings nicht bloß um eine Klarstellung (S. 63), sondern durchaus um eine Erweiterung bestehender Befugnisse zur Identitätsfeststellung. In Bezug auf ausgeschriebene Fahrzeuge war bisher nur deren Durchsuchung möglich; zugleich wird nun mit der Änderung in § 28 Nr. 6 SächsPVDG die Durchsuchung auch der Sachen der im entsprechenden Fahrzeug befindlichen Personen ermöglicht.

Zusätzlich wird angeregt, als ausgleichende Maßnahme zu der Erweiterung bestehender Befugnisse zur Identitätsfeststellung das in Abs. 1 Satz 2 enthaltene Recht einer betroffenen Person, ihr auf Verlangen unverzüglich eine Bescheinigung über die Identitätsfeststellung und deren Grund auszustellen, über den Fall von Satz 1 Nr. 2 („gefährlicher Ort“) hinaus auf weitere Kontrollsituationen zu erweitern – darunter im Mindesten die Identitätsfeststellung im Zusammenhang mit einem zur gezielten Kontrolle ausgeschriebenen Fahrzeug, mit Kontrollstellen und mit Kontrollbereichen – und überdies die jeweils betroffene Person auf dieses Recht hinzuweisen.

Zu § 19 (Maßnahmen zum Schutz vor häuslicher Gewalt und sonstigen Nachstellungen)

Mit der weitgehenden Neufassung von § 19 werden vor dem Hintergrund des Schutzes vor häuslicher Gewalt die bisher bestehenden Möglichkeiten von Wohnungsverweisung, Rückkehr- und Kontaktverbot im neuen Abs. 1 Nr. 2a um ein Annäherungs- und Aufenthaltsverbot in einem bestimmten Umkreis, im neuen Abs. 1 Nr. 2b um ein Betretungsverbot für regelmäßige Aufenthaltsorte gefährdeter und ihnen nahestehender Personen, im neuen Abs. 1 Nr. 2c um ein (Fern-)Kontaktverbot zu gefährdeten Personen sowie im neuen Abs. 1

Nr. 2d um ein Verbot des Herbeiführens eines Zusammentreffens erweitert bzw. dahingehend ausdifferenziert. Mit der Anknüpfung an die „gemeinsam mit der gefährdeten Person genutzten Wohnung“ erfolgt gegenüber der bisherigen Fassung („ihrer Wohnung“) eine Anwendbarkeit auf bisher nicht berücksichtigte Konstellationen. Zugleich wird die Eingriffsschwelle von einer gegenwärtigen auf eine konkrete Gefahr für bestimmte Schutzgüter gemindert, zu denen nunmehr auch – dies analog zum Gewaltschutzgesetz – die sexuelle Selbstbestimmung gehört.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, dem Entwurfsstand begegnen keine Bedenken. Vielmehr unterstützt die Fraktion Die Linke die Neuregelung, insbesondere auch im Hinblick auf die in der Begründung vorgenommene Anknüpfung an die Istanbul-Konvention sowie die Inbezugnahme der Definition des Begriffs „häusliche Gewalt“ gemäß des BKA-Bundeslagebilds. Lediglich klarstellend sollte in Abs. 1 Satz 3 bei der Regelung, dass die Maßnahmen nach Satz 1 mit dem Ablauf des 14. Tages nach ihrer Anordnung enden, das Wort „spätestens“ ergänzt werden. Zusätzlich wird angeregt, die in Abs. 2 enthaltene Unterrichtung der gefährdeten Person über Beratungsangebote dahingehend auszuweiten, dass die Polizei auch die Person, von der die Gefahr ausgeht, über täterorientierte Beratungsangebote informieren soll.

Zu § 21 (Aufenthaltsanordnung und Kontaktverbot)

Mit der weitgehenden Neufassung von § 21 werden die bestehenden Befugnisse zur Erteilung eines Aufenthalts- oder Kontaktverbots geändert. Bezog sich die tatortbezogene Untersagung des Aufenthalts bisher auf ein Gemeindegebiet oder einen Gemeindegebietsteil, handelt es sich nunmehr in Abs. 1 um die Untersagung des Betretens und des Aufenthalts an einem bestimmten Ort, in einem bestimmten Gebiet innerhalb einer Gemeinde oder in einem Gemeindegebiet.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, dem Entwurfsstand begegnen keine Bedenken. Zu bemerken ist allerdings, dass die bislang für Aufenthaltsverbote nach § 21 Abs. 1 auf drei Monate begrenzte Höchstfrist künftig entfallen soll. In der Begründung wird das ohnehin bestehende zeitliche Beschränkungserfordernis des Aufenthaltsverbots in Verbindung mit als typisch angesehenen Anwendungsfällen für ausreichend erachtet (S. 65). In- des sind atypische Fälle von der Anwendung der Befugnis nicht ausgenommen. Daher wird angeregt, die bisher bestehende 3-Monats-Höchstfrist für

Aufenthaltsverbote nach § 21 Abs. 1 weiterhin gesetzlich zu normieren, um weiterhin atypischen Fallkonstellationen Rechnung tragen zu können.

Zu § 28 (Durchsuchung von Sachen)

Die Änderungen in § 28 Nr. 6, 7 und 8 dienen der Umsetzung von Art. 37 Abs. 5 VO (EU) 2018/1862 und sind insoweit eine erforderliche Regelung zu polizeilichen Befugnissen, wenn eine Person, die zur gezielten Kontrolle ausgeschrieben ist, angetroffen wird. Aus dem neuen § 28 Nr. 7 folgt dabei, dass – was i. V. m. der Änderung in § 15 Abs. 1 Nr. 5 zu betrachten ist – auch die Sachen von Personen durchsucht werden dürfen, die sich in einem entsprechenden Fahrzeug befinden. Aus dem neuen Nr. 8 folgt, dass ein Fahrzeug durchsucht werden kann, das zur gezielten Kontrolle ausgeschrieben ist, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Durchsuchung zur Abwehr einer Gefahr erforderlich ist.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, dem Entwurfsstand begegnen keine Bedenken. Im Sachzusammenhang wird jedoch auf die Umsetzung der o. g. Anregung zu § 15 verwiesen.

Zu § 40 (Begriff und Mittel des unmittelbaren Zwangs, hier: Taser)

Mit der Änderung in Abs. 4 Satz 2 wird die bislang auf Spezialeinheiten beschränkte Verwendung von „Vorrichtungen für den Abschuss besonderer Formen von Projektilen [...], die darauf ausgerichtet sind, die betroffene Person zu überwältigen, ohne sie dabei tödlich zu verletzen“, aufgehoben. Damit wird der Einsatz von Distanzelektroimpulsgeräten (DEIG) oder sog. Tasern unter der Voraussetzung der Zulassung durch das SMI ausgeweitet auf den gesamten Polizeivollzugsdienst.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, dem Entwurfsstand begegnen jedoch erhebliche Bedenken.

Anzuerkennen ist unter dem Gesichtspunkt konkreter Schusswaffenprävention der polizeifachliche Bedarf nach einer Distanzwaffe, die geeignet ist, einen gegenwärtigen Angriff unverzüglich zu stoppen, ohne dass sich der Einsatz der Schusswaffe erforderlich macht. Nicht gefolgt werden kann dabei jedoch der in der Begründung aufgestellten Behauptung, Erfahrungen aus anderen Bundesländern würden zeigen, dass bereits die Androhung der Anwendung von DEIG „deeskalierend“ wirke: Nach dem gewöhnlichen Begriffsverständnis beruht Deeskalation auf einer defensiven Einsatztaktik, nicht in der

Abschreckungswirkung durch Androhen eines – vielmehr eskalativen – Waffeneinsatzes. Die Fraktion Die Linke bedauert es ferner, dass die Begründung eine Auseinandersetzung mit rechtspolitischen Bedenken und mit der Studienlage über Verletzungsrisiken insbesondere für Risikogruppen gänzlich meidet (vgl. z. B.: <https://verfassungsblog.de/polizei-und-taser/>). Dies dahingestellt, ist der Gesetzestext in mehrerlei Hinsicht unzureichend und daher zwingend zu ändern.

So wird bislang die Art der Waffe nicht spezifiziert, sondern nur aus der Begründung ergibt sich, dass „bspw. Distanz-Elektroimpulsgeräte bzw. Taser“ (S. 66) gemeint sind. Die unbestimmte Nomenklatur als „Vorrichtungen für den Abschuss...“ und die lediglich „beispielsweise“ Aufzählung von DEIG lässt auch andere Arten von Waffen als vorstellbar erscheinen. Das Regelungsziel ist normenklar dadurch abzusichern, dass DEIG im Gesetzestext konkret bezeichnet werden. Davon ausgehend, dass es definitorisch auf den „Abschuss“ ankommt, ist dabei zugleich die Anwendung im sog. Kontaktmodus, d. h. als unmittelbar an den Körper gehaltener „Elektroschocker“, auszuschließen. Darüber hinaus werden zu DEIG, anders als zu Schusswaffen, schlechterdings keine besonderen Bestimmungen getroffen; sie stehen – buchstäblich – in einer Reihe mit dem Schlagstock. Aufgrund der nicht unerheblichen Verletzungsrisiken ist es notwendig, Anwendungsvoraussetzungen zu normieren, die den DEIG zum „vorletzten Mittel“ qualifizieren und sich daher an den Bestimmungen zum Schusswaffengebrauch der §§ 43 bis 45 orientieren sollten (z. B. Einsatz gegen Personen nur, um diese angriffs- oder fluchtunfähig zu machen, vgl. § 43 Abs. 2 Satz 1; Ausschluss von Kindern und ggf. weiteren Risikogruppen, vgl. § 43 Abs. 3 Satz 1). Wie bei Schusswaffen ist zudem der Gebrauch ohne vorherige Androhung nur dann zu erlauben, wenn das zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben erforderlich ist (§ 41 Abs. 3) – was im Übrigen der Annahme in der Begründung entspricht, dass i. d. R. die Androhung genüge, also es gerade auf sie ankomme.

Zusätzlich wird angeregt, im Hinblick auf die Abschreckungswirkung von DEIG sie als Ausstattung bei Einsätzen im Schutzbereich des SächsVersG grundsätzlich zu untersagen; dies noch dazu, da Anwendungsvoraussetzungen für den Einsatz gegen Personen in Menschenmengen weder bestimmt wurden, noch vorgesehen sind. Darüber hinaus sollte die zu § 40 Abs. 4 Satz 2 i. V. m. Abs. 5 vorgesehene Evaluationspflicht ausdrücklich auch auf eine etwaige Deeskalationswirkung erstreckt werden. Die Vorlage der Ergebnisse bis spätestens 31. Dezember 2029 lässt es schließlich uneinsichtig werden, warum die Befristung der Norm mit dem geänderten § 108 auf den 31. Dezember 2031

festgelegt wurde und damit DEIG auch für den Fall, dass die Evaluierung gegen eine Verlängerung der Frist sprechen sollte, noch für längere Zeit in Gebrauch bleiben können. Mithin sollte diese Frist auf den 31. Dezember 2030 vorgezogen werden. Es verbliebe für den Gesetzgeber gleichwohl ausreichend Zeit, sich mit den Ergebnissen der Pilotierungsphase auseinanderzusetzen und die Vor- und Nachteile entlang von Praxiserkenntnis abzuwägen.

Zu § 57 Abs. 4 bis 8 (Offener Einsatz technischer Mittel zur Bild- und Tonaufnahme und -aufzeichnung, hier: Bodycams in Wohnungen)

Mit der Neufassung in den Regelungen in § 57 Abs. 4 bis 8 wird die Befugnis zum Einsatz einer Bodycam auf Wohnungen erweitert und damit nicht länger auf öffentlich zugängliche Bereiche beschränkt. Zulässig soll der Einsatz in Wohnungen sein, wenn dies mit hinreichender Wahrscheinlichkeit zur Abwehr einer dringenden Gefahr für Leib oder Leben der eigenen oder einer dritten Person erforderlich ist. Zugleich wurden in Abs. 4 Satz 1 und 2 die Anforderungen an das sog. Pre-Recording sowohl in öffentlich zugänglichen Bereichen, als auch in Wohnungen geregelt. Aus Abs. 5 Satz 2 ergeben sich die Anforderungen an die Aufzeichnung innerhalb von Wohnungen unter der Voraussetzung der dringenden Gefahr für Leib oder Leben und aus Abs. 6 Satz 2 bis 6 der dabei zu berücksichtigende Kernbereichsschutz. Aus Abs. 8 Satz 6 ergibt sich schließlich, dass die weitere Verarbeitung von in Wohnungen aufgezeichneten Daten nur nach richterlicher Feststellung der Rechtmäßigkeit der Maßnahme zulässig sein soll.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, der aktuelle Entwurfsstand bedarf jedoch Änderungen. Die Fraktion Die Linke begrüßt die Neuregelung im Hinblick auf die Nutzung etwa im Zusammenhang mit Wohnungsverweisungen in Fällen häuslicher Gewalt. Sie begrüßt ferner, dass die im *Bericht der Staatsregierung zur Evaluation von §§ 21, 61, 57 und 58 SächsPVDG* (Drucksache 8/3914) enthaltene Empfehlung für eine Verpflichtung zur Information betroffener Personen über das Recht auf Einsichtnahme in Bodycam-Aufzeichnungen in Abs. 8 Satz 4 aufgenommen wurde. Nicht nachvollziehbar erscheint hingegen die in der Begründung aufgestellten Behauptung, der Bodycam komme eine deeskalierende Wirkung zu: Der vorgenannte Bericht trägt diese Annahme gerade nicht und zieht sie bei der Konfrontation mit alkoholisierten Personen und BtM-Nutzer*innen sogar in Zweifel (ebd., S. XV). Dies

dahingestellt, berücksichtigt der Gesetzestext den besonderen verfassungsrechtlichen Schutz der Unverletzlichkeit der Wohnung unzureichend und ist daher zwingend zu ändern.

So soll zum einen das Pre-Recording nach Abs. 4 Satz 2 nicht erst beim Vorliegen einer dringenden Gefahr für Leib oder Leben, sondern bereits bei einer hinreichenden Wahrscheinlichkeit zulässig sein. Für diese Abminderung besteht kein Grund: Auch wenn mittels Pre-Recording ausgelöste Aufzeichnungen nur kurzzeitig gespeichert werden, handelt es sich um eine Einschränkung der Unverletzlichkeit der Wohnung gem. Art. 30 Abs. 3 SächsVerf, was eine – im Entwurf nicht näher begründete – Absenkung der Eingriffsschwelle gerade nicht indiziert. Zum anderen wird mit der Neuregelung der Kernbereichsschutz befugnispezifisch zwar für den Einsatz von Bodycams in Wohnungen implementiert (Maßnahmenunterbrechung, Verwertungsverbot, Löschungsverpflichtung). Jedoch gilt der Kernbereichsschutz nicht nur in Wohnungen; auch dahingehend ist der Entwurf zu ändern.

Zusätzlich wird angeregt, die zu § 57 Abs. 4 Satz 2 und Abs. 5 Satz 2 i. V. m. Abs. 11 vorgesehene Evaluationspflicht ausdrücklich auf die angenommene Deeskalationswirkung zu erstrecken. Darüber hinaus sollte aus Anlass der Erweiterung der Befugnis zur Bodycam-Nutzung der Vorschlag des Sachkundigen Prof. Dr. Hartmut Aden in der Anhörung des Innenausschusses des Sächsischen Landtags am 17.05.2024 zum damaligen – u. a. auch die Bodycam betreffenden – Gesetzentwurf der Staatsregierung zum Ersten Gesetz zur Änderung des Sächsischen Polizeivollzugsdienstgesetzes (Drucksache 7/16247) geprüft werden, die Regelungen dahingehend zu ergänzen, dass Betroffene polizeilicher Maßnahmen und anwesende Dritte das Recht erhalten, das Einschalten einer vorhandenen Bodycam zu verlangen (Apr 7/01-50 A, S. 3 sowie Anl. 2, S. 2). Bei derselben Gelegenheit sollte ebenfalls dem Vorschlag des Sachkundigen Prof. Dr. Hartmut Aden gefolgt werden, gesetzlich klarzustellen, dass eigene Bild- und Tonaufnahmen eines Einsatzes angefertigt werden dürfen und dies durch Polizeivollzugsbeamtinnen und -beamte hinzunehmen ist, so lange ein Einsatz dadurch nicht behindert wird und § 201 StGB unberührt bleibt.

Zu § 57 Abs. 9 (Offener Einsatz technischer Mittel zur Bild- und Tonaufnahme und -aufzeichnung, hier: Drohnen zur Unfallverhütung)

Mit dem neuen § 57 Abs. 9 erfolgt eine Befugnisserweiterung des offenen Einsatzes technischer Mittel zur Bildübertragung und -aufzeichnung zur Verhütung einer besonders sicherheitsrelevanten Verkehrsordnungswidrigkeit, hier die unerlaubte Nutzung elektronischer Geräte während der Fahrt gem. § 23 Abs. 1a StVO („Handy am Steuer“).

Das Regelungsbedürfnis wird zurückgewiesen, der vorliegende Entwurfsstand abgelehnt. Zur Vermeidung von Wiederholungen wird vollumfänglich auf die Ausführungen im Abschnitt II.1.d verwiesen. Ergänzend ist zu betonen, dass die Verkehrsvorschrift in § 23 Abs. 1a StVO zwar fraglos der Verhütung schwerer Unfälle dient. Jedoch richtet sich die vorgesehene Befugnis nicht auf verursachende Verstöße, sondern verdachtslos und insbesondere ohne den gemäß § 46 Abs. 1 OWiG i. V. m. § 152 Abs. 2 StPO erforderlichen Anfangsverdacht auf sämtliche Verkehrsteilnehmende im Sichtbereich, denen absehbar fast sämtlich kein Verstoß vorzuwerfen sein wird. Selbst bei Feststellung eventueller Verstöße würde es sich „nur“ um Ordnungswidrigkeiten handeln. Dem gegenüber ist das hohe Eingriffsgewicht – über den hier nicht geregelten Fall der Abstands- und Geschwindigkeitsmessung hinaus muss in das Fahrzeuginnere hineingefilmt werden – nicht zu rechtfertigen und die Befugnis damit unverhältnismäßig. Dies gilt auch dann, wenn die flächendeckende Anwendung ausgeschlossen wird. Es ist darüber hinaus anzumerken, dass es sich im Hinblick auf die Anwendung der Befugnis in Kombination mit einer Drohne zugleich um eine gravierende Fehlallokation polizeilicher Ressourcen angesichts des aner kennenswert breiten Einsatzspektrums von ULS handelt. Dazu mag sehr wohl die Verkehrsüberwachung und die Einsatzunterstützung im fließenden Verkehr gehören; denkbar erscheint beispielsweise der ULS-Einsatz zur Verfolgung fliehender Fahrzeuge unter gleichzeitiger Minderung der Gefahren sowohl für nachfahrende Einsatzwagenbesatzungen wie auch für andere Verkehrsteilnehmende. Eine dahingehende Befugnis sieht der Referentenentwurf indes nicht vor.

Zu § 57 Abs. 12 (Offener Einsatz technischer Mittel zur Bild- und Tonaufnahme und -aufzeichnung, hier: Speicherfrist)

Mit dem neuen § 57 Abs. 12, in den der Regelungsgehalt des bisherigen Abs. 10 überführt wird, erfolgt die Festlegung der Aufbewahrungs- bzw. Löschfrist für Daten und daraus entstandenen Unterlagen, die nach den Abs. 2 und 3

gefertigt worden sind. Entsprechende Bildaufzeichnungen können demnach für zwei Monate gespeichert werden, auch wenn sie nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten zur Geltendmachung öffentlich-rechtlichen Ansprüche oder zum Schutz privater Rechte erforderlich sind.

Das Regelungsbedürfnis wird zurückgewiesen, der vorliegende Entwurfsstand abgelehnt. Insbesondere stimmt der Gesetzestext nicht überein mit der Begründung, wonach der neue Abs. 12 der Regelung des bisherigen Abs. 10 entspreche. Im Unterschied zum bisherigen Abs. 10 erfolgt stattdessen pauschal eine Verdopplung der Speicherfrist ohne Anlass und ohne auch nur ansatzweise ersichtlichen Grund. Im Hinblick auf die an anderer Stelle geschaffenen Datenverarbeitungsbefugnisse, die innerhalb der Aufbewahrungsfrost auch Bildaufzeichnungen nach § 57 Abs. 2 und 3 umfassen dürfen, selbst wenn sie an sich nicht erforderlich sind, ist an der bisherigen Frist unbedingt festzuhalten.

Zu § 57a (Anwendungen zur automatisierten Verarbeitung von an öffentlichen Orten und besonders gefährdeten öffentlichen Einrichtungen offen erhobenen personenbezogenen Daten)

Der neue § 57a Abs. 1 ermöglicht es, anknüpfend an Maßnahmen der öffentlichen Videoüberwachung nach § 57 Abs. 2 und 3 eine automatisierte Datenverarbeitung („intelligente Videoüberwachung“) dazu einzusetzen, um Muster zu erkennen, die etwa auf die Begehung einer Straftat oder auf das Vorhandensein einer Waffe, eines Messers oder eines gefährlichen Gegenstands hindeuten. Wird ein solches Muster erkannt, kann eine automatisierte Nachverfolgung dafür verantwortlicher Personen anhand der Kennzeichnung in – weiteren – Bildübertragungen und -aufzeichnungen vorgenommen werden. Daran anschließend wird mit § 57a Abs. 1 Satz 4 und Abs. 2 die Befugnis geschaffen, unter der Voraussetzung einer richterlichen Anordnung bei zur Nachverfolgung gekennzeichneten Personen eine biometrische Echtzeit-Fernidentifizierung anhand des Datenbestands der polizeilichen Auskunftssysteme vorzunehmen, wenn eine erhebliche gegenwärtige Gefahr für Leib oder Leben einer Person vorliegt und sofern die Abwehr dieser Gefahr auf diese Weise unbedingt erforderlich ist.

Das Regelungsbedürfnis wird teilweise anerkannt, der vorliegende Entwurfsstand abgelehnt. Zur Vermeidung von Wiederholungen wird vollumfänglich auf die Ausführungen im Abschnitt II.2 verwiesen. Nicht in Frage gestellt wird auch hier, dass polizeiliche Aufgaben, etwa das Monitoring von Bildübertragungen,

mittels KI-Anwendungen assistiert werden könnten. Dies ist etwa bei der Einzelpersonenscharfen „Nachverfolgung“ dazu manuell gekennzeichnete Personen über unterschiedliche Aufzeichnungen und Übertragungen hinweg der Fall. Gegen diese (Teil-)Befugnis erheben sich keine Bedenken.

Doch schon bei der Musteranalyse ist in Ermangelung von Angaben zum Verfahren und dessen uneinschätzbarer Zuverlässigkeit offen, ob das Regelungsziel effektiv erreicht werden kann oder sich der polizeiliche Arbeitsaufwand infolge eines hohen Anteils falsch-positiver Treffer und dem Erfordernis einer manuellen Auswertung sämtlicher möglicher Trefferfälle – woran unbedingt festzuhalten ist – nicht sogar signifikant erhöhen wird. Über die gefälligen Anwendungsbeispiele in der Begründung (S. 70) hinaus ist gleichfalls zu bedenken, dass mittels der Musteranalyse nicht nur z. B. Unkonventionelle Spreng- und Brandvorrichtungen (USBV)-verdächtige unbeaufsichtigte Gepäckstücke registriert werden, sondern sich die Befugnis auch zum Betrieb eines „Verhaltensscanners“ eignet, der das in fast allen Fällen für die Polizei vollständig irrelevante Verhalten sämtlicher Personen im Sichtbereich registriert. Ungeachtet dieser Bedenken ist darauf hinzuweisen, dass nach dem vorliegenden Entwurfsstand i. V. m. § 57 Abs. 12 auch eine retrograde Musteranalyse anhand von „alten“ Aufnahmen ermöglicht wird. Daran ist aber nicht nur kein polizeiliches Interesse erkennbar, sondern dies entspricht auch nicht dem Normenziel im Hinblick auf die Echtzeitlichkeit der Anschlussbefugnis zur Fernidentifizierung. Es muss daher geregelt sein, dass die der Musteranalyse zu Grunde gelegten Aufnahmen gleichfalls nur echtzeitlich oder jedenfalls so zeitnah wie technisch möglich verarbeitet werden dürfen.

Bei der Echtzeit-Fernidentifizierung wiederum wird das Merkmal der Echtzeitlichkeit mit der Bestimmung in § 57a Abs. 2 Satz 3, wonach die Durchführung „zeitlich [...] auf das unbedingt erforderliche Maß zu begrenzen“ ist, tatsächlich entgrenzt. Nicht nur ist dieses Maß unbestimmt; sondern auch dieser Maßnahme könnten im äußersten Fall (nämlich i. V. m. § 57 Abs. 12) wochenalte Aufnahmen zu Grunde gelegt werden. Dies wäre aber widersinnig aufgrund des vorausgesetzten Vorliegens einer – woran unbedingt und im Hinblick auf die KI-VO zwingend festzuhalten ist – gegenwärtigen Gefahr. Jedoch fragt sich dann, inwieweit die Echtzeit-Fernidentifizierung zu deren Abwehr geeignet sein und darüber hinaus gemäß § 57a Abs. 1 Satz 4, Abs. 2 Satz 1 „unbedingt erforderlich“ werden kann: Bei dieser Gefahrenschwelle ist zur Abwehr das unmittelbare polizeiliche Einschreiten geboten, das der Identifizierung der gefährdenden Person in jedem Falle vorgehen dürfte. Unter dieser Annahme ist die Regelung zur Echtzeit-Fernidentifizierung keine präventive

Befugnis. Auch dies dahingestellt, erscheint aufgrund der befugnispezifischen Eingriffsintensität der in § 57a Abs. 3 vorgesehene Richtervorbehalt zwar richtig. Aber gerade die echtzeitliche Anwendung lässt annehmen, dass in der Praxis die Anordnung unter Annahme von Gefahr im Verzug üblich würde und es damit zur Verkehrung des Regel-Ausnahme-Verhältnisses käme – unter dann regelmäßiger Vermeidung des nur für den Antragsfall zu Gericht bestehenden Darlegungserfordernisses zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme.

§ 58 (Anlassbezogene automatisierte Kennzeichenerkennung)

Mit der Änderung in § 58 entsteht die Befugnis, automatisierte Kennzeichenerfassungssysteme (AKES) künftig „ohne Wissen der Person“, d. h. verdeckt durchzuführen, wie dies bereits vormals nach § 19a Abs. 1 Satz 4 SächsPolG a. F. möglich gewesen war. Zugleich kommt es mit dem neuen Abs. 1 Nr. 2 zu einer Erweiterung der Anlassfälle: Abgehend von dem bisher überwiegend im Vordergrund stehenden Grenzbezug kann der Einsatz auch erfolgen zur Verhütung von Straftaten von erheblicher Bedeutung unter den Voraussetzungen des § 15 Abs. 1 Nr. 3 in unmittelbarer Nähe zu den in § 15 Abs. 1 Nr. 3 genannten Anlagen, Einrichtungen, Gebäuden oder Objekten, soweit Tatsachen die Annahme rechtfertigen, dass dort Straftaten von erheblicher Bedeutung begangen werden sollen. Bei diesen Einrichtungen handelt es sich um Verkehrs- oder Versorgungsanlagen, Amtsgebäude und besonders gefährdete Objekte. Zugleich werden mehrere bisherige Anlassfälle (Verhinderung der Weiterfahrt mit einem gestohlenen oder abhandengekommenen Kraftfahrzeugkennzeichen sowie Verhinderung der Weiterfahrt von Kraftfahrzeugen ohne ausreichenden Pflichtversicherungsschutz) aus Verhältnismäßigkeitsgründen gestrichen.

Das Regelungsbedürfnis wird zurückgewiesen, der vorliegende Entwurfsstand abgelehnt. Auf der Grundlage des vorliegenden *Berichts der Staatsregierung zur Evaluation von §§ 21, 61, 57 und 58 SächsPVDG* ist die Notwendigkeit der Fortführung des § 58 SächsPVDG nicht indiziert (Drucksache 8/3914). Die Überprüfung des bisherigen stationären Einsatzes, um den es sich auch künftig handeln soll, hat – völlig ungeachtet der Frage nach einem künftig verdeckten Einsatz – signifikante Defizite hinsichtlich der Effektivität und Effizienz ergeben, insbesondere wegen der äußerst geringen Trefferquote, was den hohen personellen und finanziellen Aufwand nicht zu rechtfertigen vermag. Die erheblichen technischen Defizite sind demnach auch

herstellerseitig nicht nachzubessern. In der Begründung wird eine Auseinandersetzung mit dem Evaluationsbericht vollständig gemieden und im Übrigen offengelassen, ob – was zu befürchten steht – die beabsichtigte Anschaffung weiterer stationärer Anlagen auf neuerliche Anschaffungen derjenigen Technik hinauslaufen wird, die sich bereits als defizient erwiesen hat. Zuletzt ergab der *Bericht gemäß § 107 SächsPVDG über abgeschlossene Maßnahmen nach § 21 Absatz 2 und 3 SächsPVDG, § 57 Absatz 4 und 5 SächsPVDG, §§ 58 bis 69 SächsPVDG und § 90 SächsPVDG und Bericht nach § 2 SächsKontrollG für die im Kalenderjahr 2024 abgeschlossenen Maßnahmen* (Drucksache 8/4452), dass von 624 systemseitigen AKES-Treffern im Ergebnis nur 45, also gerade einmal rund 7 Prozent, zu verifizieren waren.

Der hilfsweisen Empfehlung des Evaluationsbericht zum vielmehr mobilen AKES-Betrieb (wie vormals nach § 19a Abs. 1 SächsPolG a. F.) wird mit dem vorliegenden Entwurf keine Folge gegeben. Die Fortführung der Befugnis und die Ausweitung über die bisherige Pilotierung hinaus erscheint demnach als evidenzwidrige Maßnahme und als (fortgesetzte) gravierende Fehlallokation polizeilicher Ressourcen.

§ 61 (Elektronische Aufenthaltsüberwachung)

Mit der Änderung in § 61 soll durch den neuen Abs. 1 Nr. 1 die Befugnis zum Einsatz der sog. elektronischen Fußfessel ausgeweitet werden auf Zwecke der 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. Zu den weiteren Änderungen gehört, dass nach dem bisherigen Abs. 7 Satz 3 die Erstellung eines Bewegungsbilds nur zulässig sein soll, wenn dies richterlich in der Anordnung besonders gestattet wird, was künftig noch im Rahmen von Maßnahmen nach Abs. 1 Nr. 1 oder 2 erforderlich sein soll, aber nicht mehr im Falle terroristischer Straftaten nach Nr. 3.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, der aktuelle Entwurfsstand bedarf jedoch Änderungen. Die Fraktion Die Linke begrüßt die Neuregelung im Hinblick auf die Ausrichtung auf Hochrisiko-Fälle von häuslicher Gewalt und Stalking. Ungeachtet dessen ist das bisher bestehende Erfordernis der richterlichen Anordnung eines Bewegungsbildes im Falle terroristischer Straftaten weiterhin gesetzlich zu normieren. Der Richtervorbehalt dient der Sicherstellung einer fallspezifischen Übereinstimmung des Überwachungszwecks mit der konkreten Maßnahme, zu der ggf. auch die Erstellung eines

Bewegungsbilds gehört; ein wesentlicher Mehraufwand entsteht daraus nicht. Da es sich zudem bei der Erstellung eines Bewegungsbilds um eine eingriffsintensivere Maßnahme handelt als die bloße Ermittlung des aktuellen Aufenthaltsorts, muss eine Änderung dahingehend erfolgen, dass das Erstellen eines Bewegungsbilds gegenüber der punktuellen Erhebung des Aufenthaltsorts unter erhöhten Anforderungsvoraussetzungen steht.

Zusätzlich wird angeregt, die Regelung so auszugestalten, dass bei Maßnahmen der elektronischen Aufenthaltsüberwachung in geeigneten Fällen Datenverarbeitungs (DV)-Technik zum Schutz vor häuslicher Gewalt mit der Möglichkeit der Ermittlung dynamischer geografischer Sperrzonen und der automatisierten Alarmierung der zu schützenden Person vor einer unerlaubten Annäherung („spanisches Modell“) eingesetzt werden kann.

Zu § 62a (Anlassbezogene Anwendung zur automatisierten Datenanalyse)

Mit dem neuen § 62a wird eine neuartige Befugnis zur anlassbezogenen automatisierten Datenanalyse geschaffen. Der Zweck liegt nach Abs. 1 Satz 1 in der automatisierten Gewinnung neuer Erkenntnisse, wobei die Datenanalyse über den sogenannten einfachen Datenabgleich, bei dem eine Suche nach z. B. einer Person parallel in mehreren Datenbeständen erfolgt, insoweit hinausgeht, dass eine Datenfusion – d. h. die Zusammenführung, Verknüpfung und Auswertung von Datenbeständen auf einer separaten Analyseplattform – vorgenommen wird.

Das Regelungsbedürfnis wird teilweise anerkannt, der vorliegende Entwurfsstand abgelehnt. Zur Vermeidung von Wiederholungen wird vollumfänglich auf die Ausführungen im Abschnitt II.1.c – zur Erforderlichkeit einer speziellen Datenverarbeitungsbefugnis zu Zwecken der automatisierten Datenanalyse – sowie im Abschnitt II.2 verwiesen. Nicht in Frage gestellt wird auch hier, dass polizeiliche Aufgaben, etwa die personenorientierte Informationsauswertung, mittels KI-Anwendungen assistiert werden könnten. Gegen den konkreten Normentwurf erheben sich jedoch erhebliche Bedenken: Es handelt sich vorliegend um eine eingriffsintensive heimliche Überwachungsmaßnahme, die auch bereits im Vorfeld einer konkretisierten Gefahr eingesetzt werden kann und darf, wofür weder der Vorbehalt einer richterlichen Anordnung vorgesehen ist, noch eine Benachrichtigungspflicht im Anschluss entsteht. Zwar würden rechtmäßig gespeicherte Daten den Ausgangspunkt der Plattformnutzung bilden. Darüber hinaus dürften in die Datenanalyse aber fast ausnahms-

los alle der Polizei vorliegenden – und weitere für sie erreichbare – Daten einbezogen werden, eingeschlossen Daten von Dritten sowie eigens für die Anwendung nacherhobene Internetdaten und nachbeschaffte Daten, die einem „Behördenwechsel“ unterlagen; lediglich Daten aus einer Wohnraumüberwachung sind ausdrücklich ausgeschlossen.

Abgesehen von Verkehrsdaten fehlen Regelungen zur Löschung personenbezogener Daten in der Analyseplattform, nachdem sie dort verarbeitet worden sind. Das gesamte Verfahren ist damit nicht nur unzureichend normiert, sondern lässt alle üblichen rechtsstaatlichen Konturierungen vermissen, wozu auch konkrete wirksame eingriffsminimierenden Vorkehrungen gehören würden. Ihrer bedürfte es, um der sonst drohenden, in ihren Auswirkungen unkalkulierbaren Uferlosigkeit sowohl der Datenverarbeitung selbst, als auch dazu vorgenommener ergänzender Datenerhebungen vorzubeugen.

Zu § 62b (Anlassbezogener nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet)

Mit dem neuen § 62b wird eine neuartige Befugnis zum anlassbezogenen nachträglichen automatisierten Abgleich biometrischer Daten zu Gesicht und Stimme mit öffentlich zugänglichen Daten aus dem Internet geschaffen.

Das Regelungsbedürfnis wird teilweise anerkannt, der vorliegende Entwurfsstand abgelehnt. Zur Vermeidung von Wiederholungen wird vollumfänglich auf die Ausführungen im Abschnitt II.2 verwiesen. Nicht in Frage gestellt wird auch hier, dass polizeiliche Aufgaben, etwa die Personenidentifizierung, mittels KI-Anwendungen assistiert werden könnten. Gegen den konkreten Normentwurf erheben sich jedoch schwerste Bedenken. Insbesondere ist unklar, ob das biometrische „Erkennungssystem“ überhaupt legal betrieben werden könnte. Denn es soll weder bloß innerhalb eines geschlossenen Katalogs polizeieigener, rechtmäßig erhobener und gespeicherter Daten eingesetzt werden, noch beschränkt sein auf eine einfach Online-Rückwärtssuche zum Auffinden übereinstimmender Dateien.

Vielmehr handelt es sich um ein ähnlichkeitsbasiertes Matching: Der dabei durchgeführte Abgleich kann jedenfalls dann, wenn Ergebnisse in einem vertretbaren Zeitraum erwartet werden, nicht schlicht gegenüber „Daten aus dem Internet“ erfolgen, sondern gegenüber daher stammender, aber bereits biometrisch vorverarbeiteter Daten in einer katalogartigen Datenbank. Nicht nur stammt das dabei indizierte Vergleichsmaterial aus praktisch unbeschränkten

privaten Datenbeständen, sondern kann dabei auch jede irgendwo abgebildete Person einem biometrischen Abgleich unterliegen. Kommerzielle Anbieter, die derartige Dienstleistung für rechtsstaatlich desinteressierte Behörden sowie für Privatanwenderinnen und -anwender zur Verfügung stellen, sind auch aufgrund der Unvereinbarkeit mit der KI-VO üblicherweise außerhalb bundesdeutscher und europäischer Jurisdiktion ansässig. Die ggf. auch über einen Drittanbieter vermittelte Nutzung einer biometrischen Vorratsdatenbank durch die Polizei Sachsen wäre als Inanspruchnahme einer verbotenen Dienstleistung zur biometrischen Rasterfahndung voraussichtlich eklatant rechts- und verfassungswidrig. Mangels jeglicher Konturierung des Verfahrens ist dies nach dem vorliegenden Entwurfsstand jedenfalls nicht auszuschließen.

Darüber hinaus ist kritisch darauf hinzuweisen, dass die Durchführung in Fällen des Abs. 1 Satz 1 zwar mit Abs. 3 Satz 1 unter den Vorbehalt einer richterlichen Anordnung gestellt und an das Vorliegen einer konkretisierten Gefahr im Hinblick auf schwere Straftaten geknüpft ist. Jedoch sind durch den in Abs. 1 Satz 2 Nr. 1 enthaltenen Verweis auf § 100a Abs. 2 StPO auch bereits „einfache“ Straftaten umfasst.

Zu § 64 (Einsatz einer V-Person, Verdeckte Ermittlerin und Verdeckter Ermittler)

Die Neufassung von § 64 trägt insbesondere verfassungsgerichtlichen Vorgaben zur Gewährleistung des Kernbereichsschutzes auf der Erhebungs-, Auswertungs- und Verwertungsebene Rechnung.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, der aktuelle Entwurfsstand bedarf jedoch Änderungen. Die Fraktion Die Linke begrüßt die vorgenommenen Änderungen ungeachtet ihrer sonstigen Vorbehalte gegen den VP-Einsatz. Bei der Gelegenheit der Änderung ist es jedoch erforderlich, ähnlich wie in § 12 Abs. 2 SächsVSG Voraussetzungen und Ausschlussgründe für die Anwerbung/Verpflichtung und für den Einsatz von VP zu normieren. Diese bislang kaum ausgeprägten Kriterien sollten jedenfalls nicht niedriger liegen als im Verfassungsschutzbereich, da – im Unterschied zu diesem – der polizeiliche VP-Einsatz bzw. daraus gewonnene Informationen zu anschließenden polizeilichen oder strafrechtlichen Zwangsmaßnahmen führen können. Insbesondere sollte der Einsatz von Personen als VP ausgeschlossen werden, die mittels Zuwendungen für ihren Einsatz den eigenen Lebensunterhalt bestrei-

ten. Darüber hinaus ist es zur effektiven Gewährleistung des Kernbereichsschutzes in § 64 Abs. 4 erforderlich, bei VP die Ausnutzung intimer/sexueller Beziehungen zur Informationsgewissen sowie bei VE das Eingehen intime/sexuelle Beziehungen im Normtext ausdrücklich zu untersagen.

Zu § 66 (Überwachung der Telekommunikation, hier: Quellen-TKÜ)

Mit dem neuen § 66 Abs. 2 wird eine Befugniserweiterung zur sog. Quellen-Telekommunikationsüberwachung vorgenommen. Wie die bisher und weiterhin mögliche konventionelle Telekommunikationsüberwachung wird die Durchführung der Quellen-TKÜ mit § 66 Abs. 4 Satz 1 unter den Vorbehalt einer richterlichen Anordnung gestellt.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, der aktuelle Entwurfsstand bedarf jedoch Änderungen. Zunächst vermag die Fraktion Die Linke nicht der in der Begründung dargelegten Auffassung zu folgen, bei der Quellen-TKÜ werde nur die Kommunikation erlangt, die auch durch eine konventionelle TKÜ erlangt würde, und als besondere Form der TKÜ liege ein Eingriff nur in das Fernmeldegeheimnis vor (S. 89). Denn über die konventionelle TKÜ hinaus findet bei der Quellen-TKÜ auf der methodisch-technischen Seite nicht nur die Ausleitung desselben – aber verschlüsselten – Rohdatenstroms statt; sondern zur Umgehung der Verschlüsselung kann die Intrusion des Endgeräts vorgenommen werden, wofür ggf. Angriffsvektoren („Sicherheitslücken“) erkannt, ausgenutzt und aufrechterhalten werden müssen, was die IT- und Datensicherheit sämtlicher Nutzer*innen gefährdet. Mithin liegt zusätzlich ein Eingriff in das IT-System-Grundrecht vor.

Bei erfolgreicher Intrusion besteht im Gegensatz zur konventionellen TKÜ nicht nur eine Zugriffsmöglichkeit auf die laufende Telekommunikation im Sinne von Telekommunikationsinhalten auf ihrem Übertragungsweg, sondern auch auf diesbezügliche – und möglicherweise darüber hinaus gehende – Daten im alleinigen Herrschaftsbereich des Betroffenen und dessen Datenspeicher. Diesem Unterschied muss der Gesetzgeber Rechnung tragen, um die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach Art. 2 I i. V. m. Art. 1 I GG zu wahren und nicht zur unerlaubten Onlinedurchsuchung überzugehen. Eben diese Grenzziehung ist im aktuellen Entwurfsstand unzureichend ausgeprägt. So ist nach Abs. 2 Satz 1 Nr. 1 zwar sicherzustellen, dass die Überwachung und Aufzeichnung ausschließlich laufender Telekommunikation erfolgt. Unmittelbar zuvor, hernach erneut in Nr. 2 sowie abermals in Abs. 2a Satz 1 ist aber von bloßer „Telekommunikation“ die

Rede. Der Unterschied wird in der Begründung noch weiter verwischt, indem dort zwar ebenfalls angeführt wird, es werde mittels Quellen-TKÜ nur „laufende Telekommunikation“ erfasst. Zugleich heißt es aber auch, erfasst werde „Kommunikation, bevor diese verschlüsselt wird“ (S. 89). Es werden damit jedenfalls gedanklich auch solche Daten dem Erhebungsbereich der Quellen-TKÜ unterworfen, die noch nicht verschlüsselt wurden und die für den Fall, dass sie noch einer Änderung unterliegen oder gar verworfen werden, als solche niemals in eine laufende Telekommunikation eingehen werden. Ein verwandtes Problem ergibt sich, wenn in der Folge der Intrusion des Endgeräts die Möglichkeit entsteht, auf gespeicherte vergangene Kommunikationsvorgänge zuzugreifen, d. h. archivierte Nachrichtenverläufe aus ehemaligen, indes nicht mehr laufenden Telekommunikationen. Ein Zugriff darauf wäre aus hiesiger Sicht gleichfalls nicht erlaubt.

Es ist daher zwingend, die Befugnis zur Quellen-TKÜ unmissverständlich und durchgängig auf die laufende Telekommunikation zu beschränken. Zur Gewährleistung einer normenklaren Abgrenzung zur unerlaubten Onlinedurchsuchung ist eine Regelung aufzunehmen, wonach es untersagt ist, mögliche zukünftige, indes unversandte Telekommunikationsinhalte (Entwürfe) sowie Inhalte ehemals laufender Telekommunikationen in abgespeicherten Nachrichtenverläufen zu überwachen und aufzuzeichnen.

Zu § 70 (Erhebung von Bestandsdaten)

Die Neufassung von § 70 trägt insbesondere verfassungsgerichtlichen Vorgaben zur Bestandsdatenauskunft Rechnung. Zu den darüber hinaus gehenden Änderungen gehört es, dass nach Abs. 1 Satz 2 Nr. 2 d) die Bestandsdatenerhebung möglich ist zur Abwehr einer konkreten Gefahr für die freiheitliche demokratische Grundordnung (fdGO). Außerdem ist im Unterschied zur bestehenden Regelung eine richterliche Anordnung nicht mehr erforderlich, wenn eine Bestandsdatenauskunft zu einer IP-Adresse nach Abs. 2 eingeholt wird.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, der aktuelle Entwurfsstand bedarf jedoch Änderungen. Keine Bedenken begegnen der Anpassung der Befugnisnorm an die Rechtsprechung des Bundesverfassungsgerichts. Davon ausdrücklich auszunehmen ist jedoch die Streichung des richterlichen Anordnungserfordernisses im Falle der IP-Adresse. Auch wenn nach dem Beschluss des BVerfG vom 27.05.2020 (1 BvR 1873/13 – 1 BvR 2618/13 – Rz. 252, „Bestandsdatenauskunft II“) die IP-Bestandsdatenauskunft nicht zwingend ei-

ner richterlichen Anordnung bedarf und auch wenn nun zugleich die Eingriffsschwelle erhöht wird, ist nicht zu verkennen, dass das Gericht seinerzeit nicht von einer neuerlichen Diskussion um die Einführung der Vorratsdatenspeicherung ausging. Unter deren Bedingungen wird die IP-Bestandsdatenauskunft eine ungleich „ergiebigere“ Erhebungsmethode sein als bisher, deren Gebrauch dann aber keinem richterlichen Vorbehalt im Einzelfall mehr unterläge. Dies ist zu ändern. Mit der maßgeblichen bundesverfassungsgerichtlichen Rechtsprechung nicht in Zusammenhang steht die auch in der Begründung nicht weiter erörterte Entscheidung, nach dem vorliegenden Entwurf die fdGO einer polizeilichen Befugnis als eigenständige „Eingriffsschwelle“ zu Grunde zu legen. Zwar ist der Schutz der fdGO eine der Aufgaben der Polizei Sachsen nach § 2 Abs. 1 Satz 2. Es handelt sich jedoch mangels weiterer Qualifizierung an irgendeiner anderen Stelle des Gesetzes um kein geeignetes und konkret bestimmbares Rechtsgut im polizeirechtlichen Sinne. Vielmehr findet hier eine unsachgemäße Vermengung mit einem verfassungsschutzrechtlichen Schutzgut statt. Dies ist zurückzuweisen und die Vorschrift ersatzlos zu streichen.

Zu § 71 (Einsatz von unbemannten Luftfahrtsystemen)

Der neue § 71 enthält erstmals eine ausdrückliche Befugnis zum Einsatz Unbemannter Luftfahrtsysteme (ULS), d. h. Drohnen. Es handelt sich insoweit nicht um eine Befugnisserweiterung, sondern um die klarstellende Normierung eines Einsatzmittels, das seit längerem genutzt wird. Der bereits vorgängige Drohneneinsatz erfolgt damit zukünftig auf Grundlage einer spezialgesetzlichen Regelung. Sie eröffnet zugleich die Möglichkeit des Drohneneinsatzes in Verbindung mit der allgemeinen (offenen) Datenerhebungsbefugnis in § 56 sowie in Kombination mit (ggf. auch verdeckten) eingriffsintensiven Befugnissen unter deren jeweiligen Voraussetzungen: die Beobachtung und Aufzeichnung mittels offener Bildübertragung nach § 57 Abs. 1 bis 3 und 9 (Veranstaltungen und Ansammlungen, Kriminalitätsschwerpunkte, Verkehrsraum); die Datenerhebung durch Observation und Einsatz technischer Mittel nach § 63 Abs. 1 und 2; die Datenerhebung durch Einsatz technischer Mittel in Wohnungen nach § 65 Abs. 1; die Datenerhebung durch Telekommunikationsüberwachung nach § 66 Abs. 1 und 2 (d. i. TKÜ und Quellen-TKÜ); sowie die Datenerhebung durch den verdeckten Einsatz technischer Mittel zur Standorterhebung nach § 68 Abs. 2.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, der aktuelle Entwurfsstand bedarf jedoch Änderungen. Die Fraktion Die Linke erkennt die Schaffung einer gesonderten Befugnis und die abschließende Aufzählung zulässiger Kombinationen mit anderen Befugnissen an. Über die Regelung in Abs. 1 Satz 2 hinaus, dass die Offenheit der Maßnahmen in Fällen von Abs. 1 Satz 1 Nr. 1 – d. h. Datenerhebung nach § 56 – gewahrt sein muss, ist zwingend zu regeln, dass sie in jedem Fall zu wahren ist, wenn dies nach Maßgabe der jeweiligen Stammbefugnis vorausgesetzt wird; darunter jedenfalls auch in den mit Abs. 1 Satz 1 Nr. 2 geregelten Fällen der offene Beobachtung und Aufzeichnung mittels Bildübertragung nach § 57 Abs. 1 bis 3 und Abs. 9. Die „gleitende“ Überführung einer offenen, rein präventiven Maßnahme in eine heimliche Datenerhebung, nur weil sie luftgestützt erfolgt und daher schwer oder gar nicht erkennbar ist, wäre unter keinen Umständen hinzunehmen.

Die Fraktion Die Linke erlaubt sich außerdem den Hinweis, dass angesichts der erheblichen Zahl bereits im Besitz der Polizei befindlicher Drohnen der in der Begründung angezeigte Beschaffungsbedarf von 20 weiteren Drohnen nicht nachvollziehbar erscheint. Ebenso wenig nachvollziehbar ist der Hinweis darauf, dass dafür erforderliche Investitionskosten bereits „im Doppelhaushalt 2027/2028“ ausgewiesen seien (S. 59). Ein solcher Doppelhaushalt ist dem Sächsischen Landtag nicht bekannt.

Zu § 79 (Befugnis zur Datenverarbeitung)

Die im § 79 vorgenommen Änderungen stehen im Zusammenhang mit umfassenden Neuregelungen der Datenverarbeitungsbefugnisse in §§ 79 bis 80d. Mit dem neuen § 79 entsteht anstelle des bisher erforderlichen Rückgriffs auf eine – dafür nach hiesiger Ansicht unzureichende – Generalklausel zur Verarbeitung personenbezogener Daten eine allgemeine Datenverarbeitungs-Befugnisregelung innerhalb des SächsPVDG. Darin wiederum entsteht mit dem neuen Abs. 4 erstmals die ausdrückliche Befugnis, zum Schutz einer Person oder zur Eigensicherung von Polizeibediensteten sog. personengebundene Hinweise (PHW) zu speichern und sog. ermittlungsunterstützende Hinweisen (EHW) zu verarbeiten.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, der aktuelle Entwurfsstand bedarf jedoch Änderungen. Ungeachtet der an sich begrüßenswerten Neuregelung weist die Fraktion Die Linke auf die bestehenden und bekannten Bedenken gegen die Verwendung und Nutzung von PHW, wie z. B. „Anste-

ckungsgefahr“, „Psychische und Verhaltensstörung“, „Land- oder Stadtstreicher“ und EHW, wie z. B. „Reisender Täter“ im Hinblick auf damit verbundene Diskriminierungs- und Stigmatisierungsrisiken hin. Diese sind dann nicht hinzunehmen, wenn mit entsprechenden Zuordnungen bestimmte Eigenschaften oder Verhaltensweisen bezeichnet werden, die nicht per se polizeirelevant sind. Daher ist zu personengebundenen und ermittlungsunterstützenden Hinweisen zu bestimmen, dass diese nur verarbeitet werden können, wenn sie unbedingt erforderlich sind.

Zu § 79b (Weiterverarbeitung zu Aus- und Fortbildungszwecken, etc.)

Die im § 79b vorgenommenen Änderungen stehen im Zusammenhang mit umfassenden Neuregelungen der Datenverarbeitungsbefugnisse in §§ 79 bis 80d. Der neue § 79b enthält zweckändernde Weiterverarbeitungsbefugnisse für personenbezogene Daten durch die Polizei und die Hochschule der Sächsischen Polizei (FH). Neben Zwecken der Aus- und Fortbildung, der Statistik, des Archivwesens und der Forschung betrifft dies in Abs. 2 insbesondere die Weiterverarbeitung zum Zweck der präventiven Gefahrenvorsorge bei Personen, die Straftaten zu begehen beabsichtigen.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, der aktuelle Entwurfsstand bedarf jedoch Änderungen. So entsteht mit dem neuen Abs. 2 u. a. auch eine Weiterverarbeitungsbefugnis zum Zweck der Gefahrenvorsorge in Bezug auf die personenbezogenen Daten einer Person, bei der tatsächliche Anhaltspunkte vorliegen, dass sie beabsichtige, die Begehung von Straftaten durch andere Personen zu unterstützen, zu fördern, vorzubereiten oder zu planen. Dabei handelt es sich – als Grundlage für einen Grundrechtseingriff – um eine höchst vermittelte, kaum zu objektivierende Annahmekette. Erst nach der Begründung erschließt sich, dass das Ziel dieser Regelung in der „Weiterverarbeitung von Adressdaten von Mitgliedern der extremistischen Szene, zu denen Erkenntnisse zur Begehung politisch motivierter Straftaten vorliegen, zum Zweck der Täteransprache und der Beratung durch die Polizei im Rahmen des Aussteigerprogramms Sachsen“ liegt (S. 98). Es ist kritisch darauf hinzuweisen, dass die Polizei Sachsen über keinerlei Beratungsaufgaben in Angelegenheiten der Ausstiigsarbeit verfügt und sie auch nicht Teil des Aussteigerprogramms (APro) ist. Will die Staatsregierung dies ändern, muss sie dazu die explizite Änderung der betreffenden Gesetzesnorm vorschlagen. Aus hiesiger Sicht vorzugswürdig ist dabei die ausdrückliche Benennung der Ansprache-

regelung zum Zweck der Gefahrenvorsorge im Gesetz, die gleichermaßen tatgeneigte wie tatgefährdete und -betroffene Personen berücksichtigt, wobei im Rahmen dieser Ansprache gezielt qualifizierte Beratungsangebote – neben dem APro kommen insbesondere auch professionalisierte Opferberatungsstellen in Betracht – unterbreitet werden können, ohne aber selbst die Beratung zu leisten oder eine ungeschulte „Kaltakquise“ vorzunehmen. Die Beratungsarbeit ist allein Aufgabe professionalisierter Fachberatungsstellen.

Zu § 79c (Training und Test von lernenden IT-Systemen)

Die Änderungen stehen im Zusammenhang mit umfassenden Neuregelungen der Datenverarbeitungsbefugnisse in §§ 79 bis 80d und sind hier zudem im Zusammenhang mit den weiteren neuen KI-Befugnissen in §§ 57a, 62a, 62b zu betrachten. Der neue § 79c stellt sich dabei als eine besondere Zweckänderungsvorschrift dar: Sie enthält die Befugnis, vorhandene personenbezogene Daten der Polizei für das Trainieren und Testen von IT-Systemen weiterzuverarbeiten. Solche Daten sollen dafür ausdrücklich auch „an Dritte oder Auftragsverarbeiter“ übermittelt werden dürfen, unter Umständen ohne vorherige Anonymisierung oder Pseudonymisierung. Den Auftrags- und Drittverarbeitern kann es darüber hinaus gestattet werden, die trainierten Modelle für eigene Zwecke weiter zu nutzen, wenn sichergestellt ist, dass aus den trainierten Modellen keine Trainingsdaten abgeleitet werden können.

Das Regelungsbedürfnis wird teilweise anerkannt, der vorliegende Entwurfsstand abgelehnt. Zur Vermeidung von Wiederholungen wird vollumfänglich auf die Ausführungen im Abschnitt II.2 verwiesen. Nicht in Frage gestellt wird auch hier, dass polizeiliche Aufgaben mittels KI-Anwendungen assistiert werden könnten, denen ein spezifisches, ggf. auch mittels Echtdaten trainiertes Datenmodell zu Grunde zu legen ist. Gegen den konkreten Normentwurf erheben sich jedoch schwerste Bedenken. An die Stelle einer fallweise zu erreichenden Eingriffsschwelle wird ein per se bestehendes, rein technisches Erfordernis gesetzt. Der pauschalen Ermächtigung in Abs. 1 fehlt es an einem klaren Bezug zu konkreten polizeilichen Aufgaben im Sinne des Gesetzes. Der Verweis auf die „eigene Aufgabenwahrnehmung“ genügt dabei nicht, denn nach § 2 Abs. 5 wären davon auch solche Aufgaben mitumfasst, die sich aus dem SächsPVDG selbst nicht ergeben. Dies ist völlig unzureichend, zumal vorliegend im weitest vorstellbaren Ausmaß die zweckändernde Weiterverarbeitung de facto fast aller polizeilicher Daten ohne weitere Beschränkung erfolgen kann und soll. Diese Daten werden ihrerseits aus – auch tiefgreifendsten

– Grundrechtseingriffen resultieren, die sich im Zuge der zweckändernden Weiterverarbeitung fortsetzen und verfestigen. So wäre es nach dem Entwurfsstand z. B. möglich, innerhalb ihrer Speicherdauer Bodycam-Aufnahmen aus dem verfassungsrechtlich besonders geschützten Bereich von Wohnungen zu nutzen. Darüber hinaus werden die Bestimmungen zu den Voraussetzungen jeweiliger Datenspeicherungen und der darin enthaltenen Differenzierungen verschiedener Kategorien von Daten unterlaufen. So wird es die Anwendung der Befugnis absehbar nach sich ziehen, dass ohne erkennbare Rechtfertigung und unter Umgehung des Einwilligungserfordernisses der vorsorgenden Speicherung die Daten unbeteiligter Personen einbezogen werden.

Gänzlich ausgeschlossen muss aus hiesiger Sicht die Weitergabe solch derart sensibler Daten an Dritte sein, worin aber gerade der Kern der Befugnis liegt. Gänzlich außer Betracht gelassen sind Überlegungen dazu, ob und inwieweit dabei eine Anonymisierung oder wenigstens Pseudonymisierung im Hinblick auf den Umfang polizeilicher Datenbestände und die Datenarten, die nicht nur vergleichsweise leicht editierbares Schriftgut sind, überhaupt systematisch möglich ist. Wohl vor diesem Hintergrund soll „vorsorglich“ die Verwendung und die Weitergabe von Klardaten ermöglicht werden. Während der Begründung zufolge zwar auch hier nicht entschieden sei, welche Software eingesetzt werden solle und ob es sich nicht auch um eine Eigenentwicklung handeln könne (S. 59), wird mit dem vorliegenden Entwurfsstand nicht nur die Weitergabe von Klardaten an Dritte ermöglicht, sondern – das Regelungsziel eklatant überschießend – für diese Dritten auch die Möglichkeit geschaffen, die mittels Echtdaten trainierten Modelle für künftig quasi beliebige Zwecke außerhalb der Einflussmöglichkeiten und des Zugriffsbereichs der Polizei, möglicherweise auch außerhalb bundesdeutscher und europäischer Jurisdiktion, zu vermarkten. Ein Zuwiderhandeln der Auftrags- und Drittverarbeiter gegen die Bestimmung, Trainingsdaten zu löschen und es zu gewährleisten, dass aus trainierten Modellen keine Trainingsdaten extrahiert werden können, könnte möglicherweise nicht bemerkt werden und wäre damit praktisch „straflos“ möglich. Gänzlich ausgeblieben sind Überlegungen dazu, ob und inwieweit es überhaupt technisch möglich ist, Trainingsdaten aus dem trainierten Modell wieder zu entfernen.

Nach alledem entfernt sich die Regelung nicht nur von dem Grundgedanken digitaler Souveränität und den Bestimmungen der KI-VO, sondern im weitest vorstellbaren Ausmaß auch von polizeilichen und überhaupt rechtsstaatsgemäßen Zwecksetzungen. Insoweit ist der vorliegende Entwurfsstand angetan,

das Vertrauen in rechtsstaatliche Institutionen zu unterminieren. Die missbräuchliche Verwendung personenbezogener Daten durch Dritte ist nur und daher zwingend dadurch auszuschließen, dass ihre Weitergabe an und Weiterverarbeitung durch Dritte stringent ausgeschlossen wird.

Zu §§ 80, 80a bis 80d (Vorsorgende Speicherung von personenbezogenen Daten)

Die Änderungen stehen im Zusammenhang mit umfassenden Neuregelungen der Datenverarbeitungsbefugnisse in §§ 79 bis 80d und sind hier zudem im Zusammenhang mit der Fortspeicherung von Daten in polizeilichen Auskunftssystemen über das Ausgangsverfahren hinaus – die sog. vorsorgende Speicherung – zu sehen, die verfassungsgerichtlichen Anforderungen bislang nicht genügt. Neu geregelt wird in § 80 die vorsorgende Speicherung personenbezogener Daten zu Verurteilten, Beschuldigten, Verdächtigen und Anlasspersonen sowie in § 80a zu Zeuginnen und Zeugen, Opfern, Hinweisgeberinnen und -gebern, Kontakt- und Begleitpersonen. Darüber hinaus regelt der neue § 80b die vorsorgende Speicherung von zu Gefahrenabwehrzwecken erhobenen Daten aus einem nicht-repressivem Zusammenhang, u. a. in Bezug auf gefährdete, hilflose oder vermissten Personen, sowie der neue § 80c die vorsorgende Speicherung zu sonstigen Personen (u. a. Erziehungsberechtigten, Vormündern und Bewährungshelferinnen und -helfern), wozu bislang gar keine, auch keine weit hergeholte Rechtsgrundlage bestanden hatte. Aus dem neuen § 80d ergeben sich schließlich differenzierte Bestimmungen zur Dauer der Speicherung, den Aussonderungsprüf- und den Höchstspeicherfristen. Gegenüber der bisherigen Regelung in § 91 Abs. 3 Satz 4 gelten dabei generell und altersgruppenabhängig kürzere Aussonderungsprüffristen als bisher: für Erwachsene fünf statt maximal zehn sowie für Jugendliche drei statt maximal fünf Jahre.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, der aktuelle Entwurfsstand bedarf jedoch Änderungen. Generell zu begrüßen ist die (Neu-)Bestimmung der Voraussetzungen für eine vorsorgende Speicherung und die Verkürzung von Aussonderungsprüffristen. Im Hinblick auf diese Fristen bleibt allerdings bei § 80d Abs. 3 Satz 1 unklar, warum überhaupt an spezielle Fristen für Verurteilte gedacht wird: Aus einer zurückliegenden Verurteilung dürfte sich in der Regel keine gesteigerte Relevanz entsprechender Daten für die Erledigung polizeilicher Aufgaben ergeben; der Zweck polizeilicher Auskunftssysteme ist es nicht, das Bundeszentralregister zu ersetzen. In besonderem

Hinblick auf die Bestimmung von Speicherfristen für Verurteilte (und Beschuldigte), die Kinder sind, ist an deren Strafunmündigkeit zu erinnern, wodurch sie weder Verurteilte noch Beschuldigte sein können. Die gesetzgeberische Antizipation eines zukünftig ggf. abgesenkten Strafmündigkeitsalters wäre eine bei der Novellierung des SächsPVDG vollständig sachfremde Erwägung und wird keine Zustimmung der Fraktion Die Linke erlangen.

Zu § 84 (Datenübermittlung im innerstaatlichen Bereich)

Die Änderung betrifft in Abs. 2 Nr. 2 b die Erstreckung innerstaatlicher Datenübermittlungsbefugnisse auf öffentliche Stellen, die keine Gefahrenabwehrbehörden sind. Nach der Begründung sind damit insbesondere Finanzbehörden oder Gerichtsvollzieherinnen und Gerichtsvollzieher im Zusammenhang mit erforderlichen Vollstreckungstätigkeiten gemeint, wobei es die Übermittlung polizeilicher Erkenntnisse ermöglichen soll, von betroffenen Personen für die Bediensteten ausgehende Gefahren zu erkennen (S. 106). Eine weitere Änderung betrifft in Abs. 3 Satz 1 Nr. 4 sowie Satz 2 die Datenübermittlung an durch das Staatsministerium für Soziales zu bestimmende Beratungsstellen zum Zweck der proaktiven Kontaktaufnahme mit einer betroffenen Person, wenn Bedarf an Beratung zum Schutz vor häuslicher Gewalt besteht.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, dem Entwurfsstand begegnen keine Bedenken. Vielmehr befürwortet die Fraktion Die Linke die Neuregelung, insbesondere auch im Hinblick auf die Bekämpfung häuslicher Gewalt. Das Erreichen des Regelungsziels ist allerdings abhängig davon, dass für die einwilligungsfreie Weitergabe an private Dritte eine unstreitige datenschutzkonforme Umsetzung gefunden wird, wozu hiermit aufgefordert wird. Dies vorausgesetzt, wird zusätzlich angeregt, über den begrüßenswerten Opferschutzfokus hinaus auch die Weitergabe personenbezogener Daten einer Person, von der auf Grund tatsächlicher Anhaltspunkte die Gefahr häuslicher Gewalt ausgeht, zum Zweck der Kontaktaufnahme durch eine spezialisierte Beratungsstelle zu ermöglichen.

Zu § 84a (Öffentlichkeitsfahndung)

Der neue § 84a enthält die Befugnis, Daten und Abbildungen zu einer Person öffentlich bekannt zu geben zum Zweck der Ermittlung der Identität oder des Aufenthaltsortes oder wenn die Abwehr einer Gefahr für Leib, Leben oder Freiheit dieser Person sonst nicht möglich ist oder wesentlich erschwert wird oder wenn von dieser Person eine Gefahr für Leib, Leben oder Freiheit anderer

Personen ausgeht. Eine Rechtsgrundlage für die polizeiliche Öffentlichkeitsfahndung hatte bislang nicht bestanden, sondern nur strafprozessuale Befugnisse in §§ 131 ff. StPO.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, der aktuelle Entwurfsstand bedarf jedoch Änderungen. Mit der Durchführung einer Öffentlichkeitsfahndung geht durch die gezielte Veröffentlichung personenbezogener Daten, wozu regelmäßig auch Lichtbilder gehören, ein tiefer Eingriff in das Persönlichkeitsrecht einher. Der Gesetzgeber muss Vorkehrungen treffen, diesen Eingriff von vornherein auf das unbedingt erforderliche Maß zu begrenzen. Vor diesem Hintergrund ist der Entwurfsstand bislang ein unzureichendes Rudiment; insbesondere trifft er keine Regelungen zu Art und Umfang der Daten sowie für die Form und Frist der öffentlichen Bekanntmachung. In allen Fallvarianten ist nicht bloß von der Gefahr, sondern von der konkreten Gefahr auszugehen. Art und Umfang der zu veröffentlichenden Daten müssen sich fallspezifisch nach dem Ziel der einzelnen Maßnahme richten und sind dementsprechend so weit wie möglich zu begrenzen. Die Veröffentlichung darf ausschließlich auf der offiziellen Website der Polizei Sachsen erfolgen; keinesfalls dürfen die Daten vonseiten der Polizei in der Form eines eigenständigen Beitrags in sozialen Netzwerken veröffentlicht und verbreitet werden. Analog zu § 131b Abs. 2 StPO muss die Veröffentlichung eindeutig erkennbar machen, dass eine Person nicht beschuldigt wird; analog zu § 131c Abs. 2 StPO muss die Maßnahme, wenn sie nach einer gewissen Zeit nicht zum Erfolg führt, wieder beendet werden, einhergehend mit der unverzüglichen Depublikation.

Zur Gewährleistung der klaren Verantwortlichkeit und Verantwortungsübernahme sollte die Öffentlichkeitsfahndung unter den Vorbehalt einer Anordnung durch die Präsidentin oder den Präsidenten des Landeskriminalamtes oder einer Polizeidirektion gestellt sein.

Zu § 88 (Zuverlässigkeitsüberprüfung zum Schutz von besonders gefährdeten Veranstaltungen)

Mit der Neuregelung kann in die Zuverlässigkeitsüberprüfung künftig auch der Datenbestand des Landeskriminalamtes Sachsen (LKA) der letzten fünf Jahre, erforderlichenfalls der Datenbestand des Ausländerzentralregisters und – „so weit im Einzelfall erforderlich“ – des Landesamtes für Verfassungsschutz Sachsen (LfV) einbezogen werden. Gegenüber dem bisher praktizierten Ver-

fahren werden die einzelnen Datenverarbeitungsschritte normiert, insbesondere im Hinblick auf die Durchführung im elektronischen Verfahren und auf die neue Möglichkeit, eine Kopie des Bundespersonalausweises zum Vorgang zu nehmen.

Das Regelungsbedürfnis wird grundsätzlich anerkannt, der aktuelle Entwurfsstand bedarf jedoch Änderungen. Da die Zuverlässigkeitsprüfung extern veranlasst wird und daher in der Regel von vornherein nicht anzunehmen ist, dass die bei der Durchführung erhobenen Daten für die polizeiliche Aufgabenerfüllung relevant sind, muss über die bereits enthaltene Zweckbindung hinaus jede Form der zweckändernden Weiterverarbeitungen – im Normtext wie in der Anwendungspraxis – ausgeschlossen werden. Dies gilt auch und insbesondere für solche Daten, die erforderlichenfalls vom LfV Sachsen bezogen werden: Nur durch einen Ausschluss der über die Zuverlässigkeitsprüfung hinausgehenden Weiterverarbeitung ist die dem in der Verfassung des Freistaates Sachsen verankerten Trennungsgebot zuwiderlaufende Vermischung polizeilicher Datenbestände mit Daten aus nachrichtendienstlichen Informationssystemen zu verhindern.

IV. Zusammenfassung und Schlussbemerkungen

Aus den eingangs im Abschnitt II. dargelegten übergreifenden Erwägungen und angesichts der im vorstehenden Abschnitt III. getroffenen Bewertungen zu einzelnen Befugnisregelungen ist das Gesetzgebungsvorhaben aus Sicht der Fraktion Die Linke teilweise anzuerkennen, jedoch aktuell insgesamt nicht zustimmungsfähig. Eine abschließende Votierung kann erst nach Zuleitung des künftigen Gesetzentwurfs an den Sächsischen Landtag vorgenommen werden.

Es wird dabei erwartet, dass den vonseiten der Sächsischen Datenschutz- und Transparenzbeauftragten in ihrer Stellungahme vom 12. November 2025 an das Staatsministerium des Innern mitgeteilten und hier weitestgehend geteilten datenschutzrechtlichen Bedenken abgeholfen wird. Da zugleich nach dem vorliegenden Entwurfsstand die bestehenden Informations- und Anhörungspflichten gegenüber der Sächsischen Datenschutz- und Transparenzbeauftragten in mehreren Fällen erweitert werden (vgl. § 57a Abs. 4 Satz 2 und 3, § 62a Abs. 4 und 6, § 62b Abs. 4 und 5, § 79c Abs. 6), ist die Staatsregierung – ungeachtet hiesiger Bedenken gegen die jeweiligen Normen selbst – gehalten, die dafür erforderliche auskömmliche personelle, sächliche und

finanzielle Ausstattung der Sächsischen Datenschutz- und Transparenzbeauftragten zu gewährleisten.

Im Wege der Vorlage des Referentenentwurfs mit Schreiben des Chefs der Staatskanzlei vom 2. Oktober 2025 wurde es im Unterschied zu dem für die Verbändeanhörung verwendeten Anschreiben irritierenderweise versäumt, den Fraktionen des Sächsischen Landtags weitere, offenbar zwischen den Koalitionsfraktionen streitige Fragen zur Novellierung des SächsPVDG mitzuteilen und ebenfalls zur Stellungnahme vorzulegen.

Rein vorsorglich erklärt die Fraktion Die Linke, dass sie der (Wieder-)Aufnahme der „öffentlichen Ordnung“ als Anlassstatbestand für eine Platzverweisung im § 18 weder aktuell noch künftig zustimmen wird. Ein solcher (Rück-)Schritt würde das im Referentenentwurf zum Ausdruck kommende Paradigma einer nach den – u. a. durch Linke-Abgeordnete erstrittenen – verfassungsgerichtlichen Maßgaben vorgenommenen Einhegung des für polizeirechtliche Gefahrenabwehrmaßnahmen zugänglichen Gefahrenvorfelds durch die Wiederaufnahme eines kaum eingegrenzten und auch kaum bestimmbareren Schutzguts durchbrechen.

Dresden, den 10. Dezember 2025

Susanne Schaper
Fraktionsvorsitzende

Sächsisches Staatsministerium des Innern
Wilhelm-Buck-Straße 2
01097 Dresden

Nur per E-Mail: Landtag@smi.sachsen.de
Nachrichtlich an: konsultation@sk.sachsen.de

**Stellungnahme zum Entwurf des Gesetzes zur
Änderung polizeirechtlicher Vorschriften**

Sehr geehrter Herr Staatsminister Schuster,

vielen Dank für die Übersendung des Gesetzentwurfes. Für die SPD-Fraktion möchte ich Ihnen die beigefügte Stellungnahme bekannt geben und bitte um Berücksichtigung im weiteren Verfahren.

Für Rückfragen und den weiteren Austausch steht die SPD-Fraktion, insbesondere Albrecht Pallas als innenpolitischer Sprecher, gern zur Verfügung.

Mit freundlichen Grüßen



Henning Homann
Vorsitzender der SPD-Fraktion im Sächsischen Landtag

Anlage: Stellungnahme der SPD-Fraktion zum Entwurf des Gesetzes zur
Änderung polizeirechtlicher Vorschriften.

Henning Homann

Fraktionsvorsitzender

Sprecher für Arbeit, Digitalisierung,
Strukturwandel, Verkehr, Wirtschaft

Telefon: 0351 493 5720

E-Mail: henning.homann@slt.sachsen.de

www.henning-homann.de

Dresden, 10. Dezember 2025

Stellungnahme zum Entwurf des Gesetzes zur Änderung polizeirechtlicher Vorschriften

Zum Entwurf des „Gesetzes zur Änderung polizeirechtlicher Vorschriften“ nimmt die SPD-Fraktion im Sächsischen Landtag wie folgt Stellung und bittet um Berücksichtigung der aufgeführten Aspekte im weiteren Verfahren:

I. Allgemeines

Die SPD-Fraktion Sachsen bekennt sich zum Koalitionsvertrag zwischen CDU und SPD für die 8. Legislaturperiode des Sächsischen Landtags und den darin vereinbarten Punkten, auch in Bezug auf das Polizeirecht im Freistaat Sachsen. Für die SPD zählen sowohl der Schutz der persönlichen Freiheitsrechte als auch die Sicherheit aller Menschen in unserem Land zu den grundlegenden politischen Zielen. Es gilt, beide Interessen in einer Balance zu halten. Dieser Anspruch leitete uns bereits bei den Koalitionsverhandlungen und ist auch Richtschnur bei den vergangenen und kommenden Beratungen über die Novelle des Polizeirechts in Sachsen.

Der nun vorliegende Gesetzentwurf soll die rechtlichen Voraussetzungen schaffen, um auf die aktuellen sicherheitspolitischen Herausforderungen angemessen reagieren zu können. Gesellschaftliche Entwicklungen, wie die fortschreitende Digitalisierung, bringt neue Gefahren mit sich, die auch unser soziales und demokratisches Gemeinwesen berühren. Das zeigen u. a. die steigenden Zahlen politisch motivierter Straftaten. Deshalb ist es wichtig, unseren Rechtsstaat und die demokratischen Strukturen vor einer drohenden Destabilisierung zu schützen. Zugleich gilt es Maß und Mitte bei einer Überarbeitung der polizeilichen Rechtsnormen zu wahren - Nicht zuletzt zum Schutz der grundlegenden Freiheitsrechte der Bürgerinnen und Bürger. Denn nicht alles, was technisch möglich oder verfassungsrechtlich gerade noch zulässig ist, ist auch sinnvoll oder geboten.

Maßgeblicher Grund für die nun anstehende Novellierung des sächsischen Polizeirechts war die Entscheidung des Sächsischen Verfassungsgerichtshofs (SächsVerfGH) vom 25.01.2024, Vf. 91-II-19, nach der mehrere Normen des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG) und des Sächsischen Polizeibehördengesetzes (SächsPBG)

Albrecht Pallas

4. Vizepräsident des Sächsischen Landtages

Sprecher für Polizei, Asyl,
Datenschutz, Sport, Integration,
Kommunales, Wohnen und Bauen

Telefon: 0351 493 5116

E-Mail: albrecht.pallas@slt.sachsen.de

www.albrechtpallas.de

**Dresden,
10. Dezember 2025**

als nicht mit der Sächsischen Verfassung vereinbar erklärt wurden. Im Koalitionsvertrag wurde deshalb die zügige Umsetzung einer verfassungsgemäßen Ausgestaltung der polizeilichen Befugnisse entsprechend der höchstrichterlichen Anforderung vereinbart. Diese gilt es in der gesetzten Frist bis zum 30.06.2026 zu realisieren, da andernfalls umfassende Teile des SächsPVDG ihre Gültigkeit zu verlieren drohen, was schwerwiegende Folgen für die Arbeit der Sächsischen Polizei nach sich ziehen würde.

Ferner sind bei einer Änderung des Polizeirechts weitere einschlägige Entscheidungen des Bundesverfassungsgerichts zu berücksichtigen. Hierzu zählen insbesondere die Urteile:

- Zu den gesetzlichen Regelungen der „vorsorgenden Speicherung“ von personenbezogenen Daten, Entscheidung vom 1. Oktober 2024, 1 BvR 1160/19 (Bundeskriminalamtsgesetz II),
- zur Auskunft über Bestandsdaten von Telekommunikationsdiensten und das „Doppeltürmodell“, Entscheidung vom 27. Mai 2020, 1 BvR 1873/13 und 1 BvR 2618/13 (Bestandsdatenauskunft II),
- zur Wahrung des Kernbereichsschutzes privater Lebensgestaltung beim Einsatz von verdeckten Ermittler:innen und V-Personen, Entscheidung vom 9. Dezember 2022, 1 BvR 1345/21, sowie
- den strafprozessualen und polizeirechtlichen Ermächtigungsgrundlagen zur Quellen-Telekommunikationsüberwachung u.a., Entscheidung vom 24. Juni 2025, 1 BvR 2466/19 (Trojaner I) und 1 BvR 180/23 (Trojaner II).

Abseits der verfassungsrechtlichen Vorgaben wurde im Koalitionsvertrag zudem die Umsetzung folgender sicherheitspolitischer Maßnahmen vereinbart, die im Entwurf enthalten sind:

- die Erweiterung polizeilicher Befugnisse zur besseren Verhütung und Bekämpfung geschlechtsspezifischer Gewalt gegen Frauen und häuslicher Gewalt entsprechend der Istanbul-Konvention,
- die Prüfung einer Befugnis zum Einsatz von Bodycams durch Beamt:innen des Polizeivollzugsdienstes innerhalb von Wohnungen und Privaträumen unter Beachtung der verfassungsrechtlichen Vorgaben,
- die Einführung einer Befugnis zur sogenannten Quellentelekommunikationsüberwachung (Quellen-TKÜ) zur Abwehr erheblicher terroristischer Gefahren oder zur Verhinderung schwerster Kapitalverbrechen, bei denen der Rückgriff auf strafprozessuale Befugnisse ausscheidet; befristet auf drei Jahre mit anschließender Evaluation,
- die Prüfung des internen Einsatzes künstlicher Intelligenz in besonders belasteten Kriminalitätsfeldern (bspw. Beweismittelsichtung im Bereich Kinderpornographie) zur Entlastung der Ermittler:innen, sowie
- die Fortschreibung des SächsPBG zur Präzisierung und Vereinfachung von Verfahren und Zuständigkeiten.

Für die SPD-Fraktion hat die Herstellung eines verfassungsmäßigen Polizeirechts und die damit einhergehende Sicherstellung der polizeilichen Handlungsfähigkeit oberste Priorität. Aufgrund der zeitlichen Dringlichkeit für die Umsetzung des sächsischen Verfassungsgerichtsurteils begrüßen wir deshalb die Vorlage des Gesetzesentwurfs. Die darin enthaltene Berücksichtigung aktueller polizeifachlicher Erfordernisse, wie die Ermöglichung einer Standortübermittlung bei Notrufen, die Schaffung der Befugnis zum Einsatz und zur Abwehr von Drohnen sowie notwendige Anpassungen an EU-Recht bewerten wir positiv.

II. Änderungsbedarfe

Der Referentenentwurf enthält einige Vorschläge, über die noch abschließend beraten und entschieden werden muss.

Angesichts der durch den Sächsischen Verfassungsgerichtshof gesetzten Frist ist es nachvollziehbar, dass der Gesetzentwurf schnell in das Anhörungsverfahren und das Konsultationsverfahren überführt wurde, um so den Novellierungsprozess zügig voranzutreiben und die Perspektive der Fachverbände sowie der Fraktionen des Sächsischen Landtags bereits frühzeitig einbeziehen zu können. Die vorliegenden Verbändestellungnahmen lassen erkennen, dass die Staatsregierung und der Sächsische Landtag sich im weiteren Verfahren mit einigen Punkten erneut kritisch auseinandersetzen müssen.

Die SPD-Fraktion sieht in diesem Zusammenhang noch Klärungsbedarf bei folgenden Punkten:

1. Strafbewehrten Vorbereitungshandlung

Im Zusammenhang mit der Entscheidung des SächsVerfGH vom 25.01.2024 ergänzt der Entwurf die Begriffsbestimmungen in § 4 SächsPVDG-E unter Nr. 6 um den Begriff der „**Vorfeldstraftaten**“. Die gewählte Begrifflichkeit ist unbestimmt und nicht selbsterklärend; sie ist kein Rechtsbegriff, sondern stammt eher aus dem politischen Sprachgebrauch. Es wird deshalb im Interesse einer Normenklarheit und Anwenderfreundlichkeit gefordert, stattdessen als legaldefinierten Rechtsbegriff die Formulierung „strafbewehrte Vorbereitungshandlung“ zu verwenden. Dieser umschreibt terminologisch adäquater die adressierte, noch nicht-konkrete oder konkretisierbare Gefährdung eines Individual- oder Kollektivrechtsguts, die den Anlass für die vorgelagerte polizeiliche Gefahrenabwehr bildet, und trägt so zu einer besseren Verständlichkeit der Begriffsbestimmung bei. Der Begriff sollte daher in allen nachfolgenden Normen entsprechend ersetzt werden.

Zudem wird empfohlen, die Definition entsprechend des Formulierungsvorschlags, der sich in der Stellungnahme von Herrn Prof. Dr. Berster von der Deutschen Hochschule der Polizei findet, abzuändern. Die dort gewählte Variante ist nicht nur in rechtlicher Hinsicht eindeutiger und damit klarer formuliert, sondern ermöglicht es zugleich, die vom SächsVerfG getroffene Unterscheidung zwischen abstrakten Gefährdungsdelikten und pönalisierten Vorbereitungshandlungen stärker bei der verfassungskonformen Ausgestaltung der Rechtsnorm zu berücksichtigen. Im weiteren Verfahren sollte außerdem, wie von der Deutschen Polizeigewerkschaft in ihrer Stellungnahme gefordert, der Umfang, der unter einer strafbewehrten Vorbereitungshandlung erfassten Verhaltensweisen kritisch überprüft werden (S. 2), um eine mögliche entgrenzte Anwendung der Rechtsnorm aufgrund unzureichend bestimmter Rechtsgüter, die es zu schützen gilt, zu vermeiden.

2. Öffentliche Ordnung

Das Sächsische Staatsministerium des Inneren bittet mit dem Anhörungsschreiben vom 6. Oktober 2025 an die Fachverbände um eine Stellungnahme, ob in § 18 Satz SächsPVDG: „Die Polizei kann zur Abwehr einer Gefahr für die öffentliche Sicherheit eine Person vorübergehend von einem Ort verweisen oder ihr vorübergehend das Betreten eines Ortes verbieten (Platzverweisung)“, die Ergänzung der Tatbestandsalternative „**öffentlichen Ordnung**“ vorgenommen werden sollte.

Dieser Einschub würde unseres Erachtens zu einer beträchtlichen Erweiterung der polizeilichen Befugnis zur Platzverweisung führen. Vor dem Hintergrund der Definition der „Öffentlichen Ordnung“ nach § 4 Nr. 2 SächsPVDG wäre so ein Eingriff in die Freiheit der Fortbewegung und des Aufenthalts (Art. 2 Abs. 2 Satz 2 GG) bereits bei geringfügigen Sozialstörungen möglich, was vor dem Hintergrund der gebotenen Rechtsgüterabwägung und des Übermaßverbotes unverhältnismäßig erscheint. Daher spricht sich die SPD-Fraktion, ebenso wie der Verband der sächsischen Verwaltungsrichterinnen und -richter (VSVR, S. 1) gegen die Einfügung aus.

3. Videoüberwachung des öffentlichen Verkehrsraums

§ 57 Abs. 9 SächsPVDG-E sieht die Befugnis zur **Videoüberwachung des öffentlichen Verkehrsraums** zur Erfassung von Verstößen gemäß § 23 Abs. 1a StVO (Handynutzung am Steuer) vor, sofern laut Satz 2 „tatsächliche Anhaltspunkte bestehen, dass an bestimmten Streckenabschnitten oder Verkehrsknotenpunkten in regelmäßiger Weise gegen die genannten Vorschriften verstoßen wird oder es sich in sonstiger Weise um einen Bereich mit besonderer Unfallträchtigkeit handelt.“ Bei der Aufzeichnung darf entsprechend Satz 3 das Fahrzeug, dessen Kennzeichen, sowie „Informationen über Ort, Zeit, Fahrtrichtung und die fahrzeugführende Person“ erfasst werden.

Die SPD-Fraktion steht einer Ausweitung der Videoüberwachung des Verkehrsraums grundsätzlich skeptisch gegenüber, da es bei einer solchen Maßnahme zu einer anlasslosen und massenhaften Erhebung personenbezogener Daten kommt, die tief in das Grundrecht auf informationelle Selbstbestimmung einer Vielzahl unbeteiligter Personen eingreift.

Darüber hinaus bestehen für die SPD-Fraktion in Bezug auf die Bekämpfung von Verkehrsordnungswidrigkeiten mittels einer Ausweitung der Videoüberwachung im öffentlichen Raum Zweifel an der Verhältnismäßigkeit der Rechtsnorm. Neben grundsätzlichen Bedenken bezüglich der Art und des Umfangs der Befugnisse stellen sich uns insbesondere Fragen, die die konkrete Ausgestaltung der Rechtsnorm betreffen. So ist zunächst festzuhalten, dass die in der Begründung angeführte Anwendung der Videoüberwachung im öffentlichen Verkehrsraum zur Prävention von Ordnungswidrigkeiten keinen schlüssigen Anlass darstellt, da die Aufzeichnung und Identifizierung von Verkehrsteilnehmer:innen nur zur nachträglichen Ahndung, nicht aber zur Verhütung von Verkehrsverstößen beitragen kann. Dies ist insbesondere der Fall, wenn – wie die Sächsische Datenschutz- und Transparenzbeauftragte (SDTB) in ihrer Stellungnahme festhält – die Überwachung gemäß § 71 Abs. 1 Satz 1 Nr. 2 SächsPVDG-E „mittels Drohnen erfolgen soll“ (S. 6-7). Deren Einsatz widerspricht nicht nur der vorgesehenen „Offenheit“ der Maßnahme, sondern stellt auch mit Blick auf das von der Rechtsnorm verfolgte Ziel deren Verhältnismäßigkeit in Frage.

Bei der Begrenzung der Befugnis in Satz 2, nach der die Maßnahme nur auf Verkehrsbereiche angewandt werden soll, in denen es „in regelmäßiger Weise“ zu einer „besonderem Unfallträchtigkeit“ kommt, fehlt eine klare Bestimmung der entsprechenden Voraussetzungen für die Videoüberwachung. Wie in der Stellungnahme der Hochschule der Sächsischen Polizei (PolFH) festgestellt wird, erfahren die gewählten Formulierungen keine genauere Konkretisierung (S. 2). Des Weiteren fehlt im aktuellen Entwurf die inhaltliche Rückbindung der Maßnahme an das von der Norm umfasste Delikt, weshalb es zu einer Entkopplung der Abwehrmaßnahme von der eigentlichen Gefahrenlage kommt.

Wie die Unabhängige zentrale Vertrauens- und Beschwerdestelle für die Polizei in ihrer Stellungnahme richtig anführt, wird in der Begründung außerdem kein statischer Beleg aufgeführt, dass die Nutzung von elektronischen Geräten tatsächlich eine der Hauptunfallursachen im Straßenverkehr darstellt (S. 2-3). Um das zu lösen, müsste der Feststellung eines Unfallschwerpunkts ein Lagebild zugrunde liegen, das an diesem Ort Verstöße gegen die verbotene Handynutzung am Steuer als Hauptunfallursache dokumentiert.

Darüber hinaus ist die Dauer der Datenspeicherung nicht klar bestimmt, da Satz 4 des vorliegenden Entwurfs nur die Löschung der erhobenen Daten „unverzüglich, spätestens jedoch mit der Beendigung der Maßnahme“ vorsieht, wobei es aber keinerlei Bestimmungen hinsichtlich der Dauer der Maßnahme gibt, wodurch ebenfalls die Dauer der Datenspeicherung ungeklärt bleibt.

Die SPD-Fraktion hat daher ernste Bedenken gegen die Regelung in § 57 Abs. 9 SächsPVDG-E, die auch von der SdTb geteilt werden (S. 4ff.). In ihrer Stellungnahme zum vorliegenden Gesetzentwurf hält sie fest, dass die Vorschrift „weder den Vorgaben des Sächsischen Verfassungsgerichtshofs noch den durch das Bundesverfassungsgericht benannten verfassungsrechtlichen Anforderungen“ (S. 6) entspricht. Es wird deshalb die Streichung aus dem Gesetzentwurf empfohlen. Mindestens wird jedoch die Überarbeitung des § 57 Abs. 9 SächsPVDG-E entsprechend den Kritikpunkten zur Herstellung einer verfassungsmäßigen Ausgestaltung der Rechtsnorm gefordert.

4. Biometrischer Abgleich und automatisiertes Tracking an öffentlichen Orten

Bei der in § 57a SächsPVDG-E vorgesehene Einführung von „Anwendungen zur automatisierten Verarbeitung von an öffentlichen Orten und besonders gefährdeten öffentlichen Einrichtungen offen erhobenen personenbezogenen Daten“ bestehen für die SPD-Fraktion ebenfalls grundlegende und schwerwiegende Bedenken hinsichtlich des Umfangs, der Intensität und Tiefe der vorgesehenen Maßnahmen. So ist in § 57a Abs. 1 Satz 1 SächsPVDG-E zunächst die Befugnis geregelt, dass die Polizei Aufzeichnungen gemäß § 57 Abs. 2 und 3 SächsPVDG-E unter **Einsatz Künstlicher Intelligenz** auswerten kann, **um mögliche Muster zu erkennen**, die „auf die Begehung einer Straftat“ oder die Anwesenheit einer Waffe „im Sinne des § 1 Absatz 2 des Waffengesetzes, Messer und gefährliche Gegenstände“ in der betreffenden Situation hindeuten.

Sollte ein solches Muster erkannt und nach einer Prüfung mit einer „Straftaten von erheblicher Bedeutung in absehbarer Zeit mit hinreichender Wahrscheinlichkeit gerechnet werden“, kann gemäß § 57a Abs. 1 Satz 2-4 SächsPVDG-E eine Kennzeichnung der betreffenden Person(en) in der Aufnahme und deren automatisierte Nachverfolgung sowie ggf. eine **biometrische Echtzeit-Fernidentifizierung** bei Vorliegen einer erheblichen Gefahr veranlasst werden. Ebenso ist eine Echtzeit-Fernidentifizierung gemäß § 57a Abs. 2 SächsPVDG-E möglich, wenn sie zur Abwehr einer tatsächlichen und bestehenden oder vorsehbaren Gefahr, einer terroristischen Straftat, zum Auffinden von „Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung“ oder vermissten Personen dient.

Wir betrachten die Befugnisse nach § 57a SächsPVDG-E skeptisch, da bereits die massenhafte Erfassung von Personen durch Videoüberwachung einen Eingriff in das informationelle Selbstbestimmungsrecht einer Vielzahl von betroffenen Personen darstellt, wie das Bundesverfassungsgericht in seinem Urteil vom 16. Februar 2023 zur automatisierten Datenverarbeitung, 1 BvR 1547/19 und 1 BvR 2634/20 und das Sächsische Verfassungsgericht in seinem Urteil vom 25.01.2024, Vf. 91-II-19, festhalten. Zwar geht die Erfassung im öffentlichen Raum aufgrund der Offenheit der Maßnahme und der Öffentlichkeit des Raums nur mit einer geringfügigeren Betroffenheit der aufgezeichneten Personen einher. Durch die in § 57a Abs. 1 SächsPVDG-E vorgesehene automatisierte Auswertung zum Zwecke der Mustererkennung, sowie das sich daran möglicherweise anschließende Tracking oder den Biometrie-Abgleich, wie sie in § 57a Abs. 1 und 2 SächsPVDG-E vorgesehen sind, werden die Reichweite, die Intensivität und die Tiefe des Eingriffs allerdings massiv erhöht. Im Falle des automatisierten Trackingprozesses erhöht sich die Schwere des Eingriffs nochmals, da aus dem vorliegenden Entwurf keine zeitliche Begrenzung der Maßnahme hervorgeht. Erschwerend tritt zudem hinzu, dass der Biometrie-Abgleich im Kontext von terroristischen Straftaten auch bereits bei sog. „Vorfeldstraftaten“ sowie „strafbewerten Vorbereitungshandlungen“ Anwendung finden soll. Unseres Erachtens widerspricht der Normenentwurf an dieser Stelle klar dem Grundsatz der Verhältnismäßigkeit.

Des Weiteren stellt sich mit Blick auf die Zielstellung der Befugnis die Frage, inwiefern der bloße biometrische Abgleich gemäß § 57a Abs. 1 Satz 4 SächsPVDG-E zur Abwehr einer gegenwärtigen Gefahr dienen soll, da diese sich nicht durch die bloße Identifizierung der handelnden Person herbeiführen lässt, sondern das aktive Einschreiten von Einsatzkräften erfordern würde. Wie die SDTB in ihrer Stellungnahme festhält, lässt dies Zweifel an der Eignung der Norm und folglich auch an ihrer Verhältnismäßigkeit aufkommen (S. 9).

Unklarheiten bestehen des Weiteren hinsichtlich in § 57a Abs. 2 Nr. 2 Satz 3 SächsPVDG-E nicht eingehender erläuterten Regelung bezüglich der zeitlichen und räumlichen Begrenzung der biometrischen Echtzeit-Identifizierung sowie des generellen Regelungsinhalts der einzelnen Rechtsnormen, wie auch die PolFH in ihrer Stellungnahme anzeigt (S. 2).

Anschließend an diese Punkte ergeben sich in Anbetracht der nur überschaubaren Ergebniswerte erster Testmodelle, beispielweise des Modellversuchs am Berliner Bahnhof Südkreuz (siehe Bundespolizeipräsidium Potsdam 18.09.2018) und einer erhöhten Fehlerquote bei der Erkennung von Frauen, Kindern oder Menschen mit Migrationshintergrund aufgrund systemischer Unzulänglichkeiten der gängigen Testdaten zudem noch erhebliche Zweifel an der Einsatzfähigkeit bestehender Systeme und somit der sicheren und diskriminierungsfreien Umsetzbarkeit der Rechtsnorm. Die SPD-Fraktion spricht sich deshalb zum jetzigen Zeitpunkt gegen die Einführung des § 57a SächsPVDG-E aus.

5. Quellen-TKÜ

§ 66 Abs. 2-3 SächsPVDG-E sieht zur „Überwachung der Telekommunikation“ die Möglichkeit vor, „dass mit technischen Mitteln in die von einer betroffenen Person genutzten informationstechnischen Systeme eingegriffen wird“, um so ausschließlich deren „laufende Telekommunikation“ zu überwachen und aufzuzeichnen (**Quellen-TKÜ**).

Entsprechend der Vereinbarung im Koalitionsvertrag trägt die SPD-Fraktion die Einführung dieser Befugnis grundsätzlich mit. Wir haben allerdings noch Vorbehalte bezüglich der möglichen Anwendung einer Quellen-TKÜ in informationstechnischen Systemen von Dritten, die im Sinne des § 66 Abs. 2a Nr. 4 und 5 SächsPVDG-E unwissentlich technische Geräte oder Anschlüsse zur Kommunikation bereitstellen oder Meldungen entgegennehmen und weitergeben, die zur Begehung von Straftaten gemäß Nr. 1-3 verwendet werden. Bereits die Überwachung der Quellentelekkommunikation gemäß § 66 Abs. 2a Nr. 1 SächsPVDG-E stellt einen tiefgehenden Eingriff in das Fernmeldegeheimnis gemäß Art. 10 GG sowie das Persönlichkeitsgrundrecht gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG der betroffenen Personen dar. Dabei werden deren Recht auf informationelle Selbstbestimmung sowie das sich aus der Rechtsnorm ergebende Grundrecht auf Unversehrtheit informationstechnischer Systeme (IT-System-Grundrecht, siehe das Urteil des BVerfG vom 24. Juni 2025, 1 BvR 2466/19) eingeschränkt. Denn bei einem solchen Eingriff wird nicht nur die Vertraulichkeit und Integrität der betreffenden Systeme in Frage gestellt. Ebenso besteht die Möglichkeit, „einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten“ (Urteil des BVerfG vom 27. Februar 2008, 1 BvR 370/07 und 1 BvR 595/07, Rn. 203).

Wird die heimliche Überwachung nun auf Personen angewandt, die für eine Gefahr selbst nicht verantwortlich sind, ist bei der Abwägung der kollidierenden Rechtsgüter der Grundsatz der Verhältnismäßigkeit nochmals strenger zu berücksichtigen. Zudem lässt sich mit Blick auf die geringe Fallzahl, in denen gemäß § 100 a Abs. 1 Sätze 2 und 4 StPO in Sachsen bisher eine Quellen-TKÜ angeordnet wurde (für das Jahr 2023 bspw. nur fünf bzw. sieben angeordneten Maßnahmen für den Freistaat Sachsen, siehe die Antwort des Sächsischen Staatsministeriums für Justiz zur Drs 8/3774 vom 3. September 2025), die Frage aufwerfen, inwiefern eine wie in § 66 Abs. 2a Nr. 4. und 5 SächsPVDG-E vorgesehen weitergehende Befugnisnorm gegenüber unwissenden Dritten polizeipraktisch tatsächlich notwendig ist. In Anlehnung an das PolG NRW fordern wir deshalb, dass § 66 Abs. 2a Nr. 4. und 5 SächsPVDG-E dahingehend geändert werden, dass nur bei schwerwiegenden Gefahren gemäß Nr. 1 des § 66 Abs. 2a SächsPVDG-E eine Quellen-TKÜ gegen unwissende Dritte angewandt werden darf.

6. Auswertung personenbezogener Daten mit Hilfe künstlicher Intelligenz

Der vorliegende Entwurf sieht gemäß § 62a SächsPVDG-E die Einführung einer anlassbezogenen automatisierter **Auswertung personenbezogener Daten mit Hilfe künstlicher Intelligenz** zur Unterstützung der Arbeit der Polizeibehörden und zur Abwehr einer Reihe von Gefahren und schwerer Straftaten vor. Daran anschließend ist im § 62b SächsPVDG-E die Befugnis für einen „Biometrischen Abgleich mit Daten aus dem Internet“, sowie im § 79c SächsPVDG-E die Einführung einer Befugnis zum „Trainieren und Testen von lernenden IT-Systemen“ vorgesehen. Bei den Verhandlungen zum Referentenentwurf wurde hierbei festgehalten, dass „(d)ie Aufnahme der neuen Befugnisregelung der anlassbezogenen automatisierten Datenanalyse (§ 62a) [...] ohne Vorfestlegung auf ein bestimmtes IT-System“ erfolgt und kein Vertrag mit dem eine solche Software anbietenden Unternehmen „Palantir Technologies Inc.“ eingegangen wird.

Die SPD-Fraktion bekräftigt ausdrücklich ihre Unterstützung dieser Vereinbarung. Aufgrund schwerwiegender Bedenken gegenüber dem Unternehmen, seinem Gründer und Investoren sowie dem bestehenden Missbrauchspotenzial, das die Einspeisung enormer personenbezogener Datensätze in ein solches System und der Speicherung auf Servern außerhalb der Europäischen Union bereithält, kommt für die polizeilichen Nutzung einer solchen KI-Anwendung nur ein nationales oder europäisches Produkt in Frage, das entsprechend der Unionsregelung zum Daten- und Grundrechtsschutz entwickelt und ausgestaltet wurde.

Hinsichtlich der konkreten Ausgestaltung des IT-Systems gibt es zudem noch Fragen, die es im weiteren Verfahren zu klären gilt. Entsprechend der verfassungsgerichtlichen Vorgaben zur automatisierten Datenanalyse (Urteil des BVerfG vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20) sowie der Stellungnahme der SDTB (S. 14 ff.) sollte beispielsweise sichergestellt werden, dass es sich um ein bereits austrainiertes, determiniertes System handelt, das rechtmäßig und unveränderlich vorprogrammiert worden ist, um die hohe Eingriffsintensität der Maßnahme abzumindern. Dies würde den Einsatz eines „lernenden Systems“ ausschließen, bei dem die Daten, die zur Entwicklung und Training der KI verwendet werden und sich nicht mehr eindeutig aus dem System entfernen lassen. Dies erfordert auch, dass wie in dem Urteil des BVerfG vorgegeben, eine klare Beschränkung des automatisierten Datenabgleichs im Gesetz selbst festgeschrieben wird (a.a.O., Rn 121). Diese fehlt im aktuellen Entwurf allerdings noch.

Darüber hinaus ist die mögliche Weitergabe polizeilich erhobener Daten an Dritte, insbesondere kommerzielle Firmen in Drittstaaten, zum Training oder Testen von KI-Systemen sowie deren Verwendung für Zwecke von nicht-öffentlicher Stellen kritisch zu überprüfen, da hierbei ein Verstoß gegen Art. 59 der Europäischen KI-Verordnung droht. Zur Wahrung der Verhältnismäßigkeit bei der Anwendung der automatisierten Datenanalyse sollte zudem geprüft werden, ob die Anordnung einer automatisierten Datenanalyse entsprechend der Stellungnahme der SDTB unter einen Richtervorbehalt gestellt und eine Benachrichtigungspflicht eingeführt wird (S. 15). Ferner sollten aus Sicht der SPD-Fraktion die konkreten Verfahren einer Anonymisierung bzw. Pseudonymisierung personenbezogener Daten gemäß § 79c Abs. 2 SächsPVDG-E geklärt werden. Hierbei ist wichtig, dass ein Verfahren gewählt wird, durch das die Anonymisierungs- und Pseudonymisierungspflicht nicht unterlaufen wird. Zudem sollte eine klare Regelung bezüglich der Löschpflichten für die zusammengeführten Daten in den Normenentwurf geprüft werden, wenn sich aus diesen keine neuen Erkenntnisse zur Erfüllung der ursprünglichen Maßnahmen ergeben.

Im Vorfeld der Einführung des IT-Systems sowie während dessen Betrieb ist entsprechend der Stellungnahme des Bundes der Kriminalbeamten ferner darauf zu achten, dass die zuständigen Beamt:innen eine umfassende Ausbildung zu „Funktionsweisen, technischen Grenzen, algorithmischen Fehlerquellen und Bias-Risiken“ des Systems erhalten (S. 11). Außerdem wird empfohlen, die in der Stellungnahme angeraten „systematischen Qualitätssicherungsprozesse“, nach denen die „Analyseergebnisse stichprobenartig validiert und überprüft werden“ (ebd.) bei der Erstellung der entsprechenden Verwaltungsvorschrift oder durch eine Anpassung der Befugnisnorm zu berücksichtigen.

III. Gestaffeltes Inkrafttreten

Um eine aus polizeifachlicher Sicht reibungslose sowie rechtssichere Einführung der neugeschaffenen Befugnisse zum Mitführen und zum **Einsatz von Distanzelektroimpulsgeräten (DEIG)** durch Beamt:innen des Polizeivollzugsdienstes in den Flächendienststellen durch die Streichung der Wörter „von Spezialeinheiten“ in § 40 SächsPVDG-E zu gewährleisten, befürworten wir eine zeitlich gestaffelte Einführung der neugeschaffenen Normen.

Die Einführung des sog. Tasers für Beamt:innen außerhalb von Spezialeinheiten wird mit dessen abschreckenden Wirkung und der Möglichkeit eines abgestuften Vorgehens zur Lagebewältigung gegenüber dem direkten Schusswaffengebrauch begründet. Allerdings kann es beim Einsatz eines DEIG auch zu schwerwiegenden bis lebensgefährlichen Verletzungen kommen, insbesondere bei Vorliegen einer Herzkreislauferkrankung oder dem Konsum von Alkohol und Drogen durch die betroffene Person. Durch das DEIG können auch Risiken für die mitführenden Polizeibediensteten entstehen. Aus diesem Grund war es lange Zeit einhellige Fachmeinung, dass DEIG nur durch Spezialeinheiten genutzt werden dürfen, die regelmäßig und intensiv den richtigen und zielgerichteten Einsatz trainieren können. Durch die Erfahrung in anderen Bundesländern lässt sich inzwischen erkennen, dass der breitere Einsatz von DEIG unter den richtigen Rahmenbedingungen risikoarm, sinnentsprechend und effektiv möglich ist. Die Pilotversuche in den entsprechenden Bundesländern haben auch die polizeifachliche Debatte und Position bzgl. der Beschränkung des Taser-Einsatzes verändert. Daher unterstützen wir eine eigene sächsische Erprobung eines breiteren Einsatzes der DEIG, zunächst in zwei Polizeidirektionen. Die Erprobung ist folgerichtig mit einer Evaluationspflicht und einer gesetzlichen Befristung zu versehen.

Bevor der Einsatz der Taser in den Flächendienststellen zugelassen werden kann, müssen Polizeitrainer:innen sowie die Polizeibediensteten für den Einsatz fortgebildet werden, was selbst bei nur zwei erprobenden Polizeidirektionen einige Zeit in Anspruch nehmen wird. Es wird deshalb empfohlen, vor der flächendeckenden Einführung der DEIG im Streifendienst eine mindestens sechsmonatige Vorbereitungszeit voranzustellen, in deren Verlauf zunächst die polizeilichen Ausbilder:innen auf die Vermittlung eines sachgerechten Umgangs mit den DEIG vorbereitet werden. In einem zweiten Schritt können dann die mitführenden Beamt:innen im sicheren und adäquaten Umgang mit den Geräten unterwiesen werden. Im Ergebnis regt die SPD-Fraktion ein um ein Jahr verzögertes Inkrafttreten des Art. 1 Nr. 10 des Gesetzentwurfs über die Änderung polizeirechtlicher Vorschriften an.

Abseits der gesetzlichen Regelungen empfiehlt die SPD-Fraktion zu gewährleisten, dass im Zuge der einjährigen Einführungs- und Vorbereitungszeit den Beamt:innen ausreichend räumliche und zeitliche Trainingsmöglichkeiten bereitgestellt werden. Zusätzlich ist entsprechend der Stellungnahme der Gewerkschaft der Polizei die Ausstattung nur einzelner Beamt:innen pro Dienstgruppe mit den Geräten zu prüfen (S. 8), da sich so die hohen Anschaffungskosten pro DEIG reduzieren lassen und eine intensivere Einweisung der mitführenden Beamt:innen in die fachgerechte Bedienung der Geräte gewährleistet werden kann.

SÄCHSISCHES STAATSMINISTERIUM DER JUSTIZ
Hospitalstraße 7 | 01097 Dresden

Sächsisches Staatsministerium
des Innern
Polizeirecht@smi.sachsen.de

Ihre Ansprechperson
Frau Silke Schlosser

Durchwahl
Telefon +49 351 564-16204
Telefax +49 351 564-16209

nkr@smj.justiz.sachsen.de

Ihre Nachricht vom
30. Januar 2026

Aktenzeichen
(bitte bei Antwort angeben)
1030/176/125-NKR

Dresden,
12. Februar 2026

Entwurf des Gesetzes zur Änderung polizeirechtlicher Vorschriften
hier: Stellungnahme des Sächsischen Normenkontrollrats gemäß § 6
Absatz 1 des Sächsischen Normenkontrollratsgesetzes
(SächsNKRg)

Der Sächsische Normenkontrollrat hat den oben genannten Entwurf geprüft.

1. Zusammenfassung

Haushaltsauswirkungen davon Freistaat	2026: 888.500 Euro 2027: 914.000 Euro 2028: 1,9 Mio. Euro 2029: 3,3 Mio. Euro
davon Kommunen	keine Auswirkungen
Erfüllungsaufwand Bürgerinnen und Bürger	keine Auswirkungen
Erfüllungsaufwand Wirtschaft	keine Auswirkungen
Erfüllungsaufwand Verwaltung davon Freistaat	nicht vollständig quantifizierte jährliche Be- und Entlastungen, insbesondere Sachaufwand in Millionenhöhe für Beschaffungen
jährlicher Personalaufwand	185.000 Euro
einmaliger Personalaufwand	825.000 Euro
jährlicher Sachaufwand	3,2 Mio. Euro
einmaliger Sachaufwand	3,1 Mio. Euro
davon Kommunen	keine Auswirkungen



Hausanschrift:
Sächsisches Staatsministerium
der Justiz
Hospitalstraße 7
01097 Dresden

www.justiz.sachsen.de/smj

Verkehrsverbindung:
Zu erreichen mit
den Straßenbahnlinien
3, 6, 7, 8, 11

Parken und behinderten-
gerechter Zugang über
Einfahrt Hospitalstraße 7

Hinweise zum **Datenschutz** erhalten
Sie auf unserer Internetseite. Auf
Wunsch senden wir Ihnen diese
Hinweise auch zu.

Per E-Mail kein Zugang für elektronisch
signierte sowie verschlüsselte
elektronische Nachrichten; nähere
Informationen zur elektronischen
Kommunikation mit dem Sächsischen
Staatsministerium der Justiz unter
<https://www.justiz.sachsen.de/E-Kommunikation-SMJ>

Weitere Wirkungen	Durch die neuen Ordnungswidrigkeitstatbestände (§ 106a SächsPVDG-E) sind bei Bürgerinnen und Bürgern Geldbußen zu erwarten.
Der Sächsische Normenkontrollrat bittet um eine Anpassung der Darstellung des Erfüllungsaufwandes. Wenngleich grundsätzliches Verständnis dafür besteht, dass einzelne Angaben aufgrund ihrer prognostischen Natur nur schwer zu ermitteln sind, äußert der Sächsische Normenkontrollrat Bedenken hinsichtlich der nicht vollständigen Quantifizierung der Auswirkungen auf den Erfüllungsaufwand mehrerer technischer Befugnisnormen. Der Sächsische Normenkontrollrat bittet zudem um Überprüfung normierter Schriftformerfordernisse, insbesondere soweit die Kommunikation zwischen Polizei und Gericht betroffen ist.	

2. Im Einzelnen

2.1. Regelungsinhalt

Das zuständige Ressort passt polizeirechtliche Vorschriften, insbesondere das Sächsische Polizeivollzugsdienstgesetz (SächsPVDG), an aktuelle Gegebenheiten an. Hierbei werden das Urteil des Sächsischen Verfassungsgerichtshofes vom 25. Januar 2024 sowie mehrere grundlegende Entscheidungen des Bundesverfassungsgerichtes berücksichtigt. Die Änderungen betreffen im Wesentlichen die

- Anpassung von Eingriffsschwellen,
- Änderung von Befugnissen zur Datenverarbeitung, Datenweiterverarbeitung und Datenspeicherung,
- Stärkung des Kernbereichsschutzes auf der Erhebungs-, Auswertungs- und Verwertungsebene beim Einsatz verdeckter Ermittler und V-Personen,
- Regelung der Quellen-Telekommunikationsüberwachung,

- Ausweitung des Einsatzes von Bodycams auch auf den Bereich von Wohnungen und Privaträumen,
- Erweiterung der Befugnisse zum Schutz Betroffener vor häuslicher Gewalt,
- Erweiterung der Ausschreibungsgründe auf den der Ermittlungsanfrage,
- Schaffung einer Befugnis zur automatisierten Datenanalyse,
- Schaffung einer Befugnis zur intelligenten Videoüberwachung unter Einführung einer biometrischen Echtzeit-Fernidentifizierung,
- Schaffung einer Befugnis zum anlassbezogenen biometrischen Datenabgleich mit öffentlich zugänglichen Daten aus dem Internet,
- Aufnahme von Befugnissen zur Abwehr und zum Einsatz unbemannter Fahrzeugsysteme,
- Aufnahme einer Befugnis zur Standortdatenübermittlung bei Notrufen,
- Aufnahme einer Befugnis zur öffentlichen Ausschreibung von gefährdeten oder gefährdenden Personen,
- Umbenennung des Polizeiverwaltungsamtes in „Polizeipräsidium für Service und IT“.

2.2. Darstellung des Staatsministeriums des Innern (SMI)

Das zuständige Ressort hat umfangreiche Angaben zum Erfüllungsaufwand gemacht, wobei diese teils unter den Haushaltsauswirkungen statt bei der Darstellung des Erfüllungsaufwandes erfolgen. Für Einzelheiten wird auf die Begründung des Gesetzentwurfes verwiesen. Die Regelungen haben keine Auswirkungen auf den Erfüllungsaufwand der Bürgerinnen und Bürger, der Wirtschaft und der Kommunen. Für die Verwaltung des Freistaates Sachsen ergibt sich sowohl einmaliger als auch jährlicher Erfüllungsaufwand in Millionenhöhe.

Auf Nachfrage hat das Ressort ergänzende Angaben zum Erfüllungsaufwand gemacht.

2.3. Haushaltsauswirkungen

Entsprechend dem Kostenblatt des SMI kommt es beim Freistaat im Jahr 2026 zu Ausgaben in Höhe von 888.500 Euro, im Jahr 2027 in Höhe von 914.000 Euro, im Jahr 2028 in Höhe von 1,9 Mio. Euro und im Jahr 2029 in Höhe von 3,3 Mio. Euro.

Durch die neuen Ordnungswidrigkeitstatbestände (§ 106a SächsPVDG-E) kommt es zudem zu Einnahmen aus Geldbußen beim Freistaat Sachsen.

2.4. Erfüllungsaufwand

Das Prüfungsrecht des Sächsischen Normenkontrollrats ergibt sich aus § 4 Absatz 1 Satz 1 Nummer 1 SächsNKRK.

Hinsichtlich der Umsetzung von verbindlichem Recht der Europäischen Union entfällt das Prüfungsrecht des Sächsischen Normenkontrollrats gemäß § 4 Absatz 1 Satz 2 Nummer 2 SächsNKRK.

2.4.1. Erfüllungsaufwand für Bürgerinnen und Bürger

Die Änderungen haben keine Auswirkungen auf den Erfüllungsaufwand der Bürgerinnen und Bürger.

2.4.2. Erfüllungsaufwand für die Wirtschaft

Die Änderungen haben keine Auswirkungen auf den Erfüllungsaufwand der Wirtschaft.

2.4.3. Erfüllungsaufwand für die Verwaltung

2.4.3.1. Erfüllungsaufwand des Freistaates

Soweit eine konkrete Befugnis zum Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme („Drohnenabwehr“, § 12a SächsPVDG-E) geschaffen wird, zieht diese jedenfalls keinen Erfüllungsaufwand nach sich, da derartige Maßnahmen bisher bereits aufgrund der Generalklausel ergriffen wurden. Die Anschaffung weiterer Technik hängt nicht kausal mit der nunmehr konkreten Normierung der Befugnis zusammen.

Mit der Änderung von § 40 Absatz 4 Satz 2 SächsPVDG wird die personelle Verwendungsbeschränkung des Einsatzes von Distanzelektroimpulsgeräten („Taser“), zunächst befristet bis 31. Dezember 2031, aufgehoben. Durch die Anschaffung 120 weiterer Geräte fällt einmaliger Sachaufwand in Höhe von 324.000 Euro an. Hinzu kommt

einmaliger Personalaufwand infolge von durchzuführenden Schulungsmaßnahmen in Höhe von 463.838 Euro bei angenommener Teilnahme von 540 Beamten der Laufbahngruppe/Einstiegsebene (LG/E) 1.2 und 2.1 ([16 Stunden x 270 Bedienstete der LG/E 1.2 x 47,88 Euro Personalkostensatz je Arbeitsstunde LG/E 1.2 gemäß Anlage 2a VwV Kostenfestlegung] + [16 Stunden x 270 Bedienstete der LG/E 2.1 x 59,49 Euro Personalkostensatz je Arbeitsstunde LG/E 2.1 gemäß Anlage 2a VwV Kostenfestlegung]). Der einmalige Sachaufwand im Zusammenhang mit den Schulungen beträgt 67.997 Euro (8.640 Stunden x 7,87 Euro Sachkosten je Arbeitsstunde gemäß Anlage 2a VwV Kostenfestlegung). Darüber hinaus entsteht einmaliger Sachaufwand im Zusammenhang mit den technischen Geräten in Höhe von 1,3 Mio. Euro (219.000 Euro x 6 Jahre).

Die Befugniserweiterung zum Einsatz von Bodycams in Wohnungen (§ 57 Absatz 4 Satz 2 SächsPVDG) führt zu nicht quantifizierten Be- und Entlastungen einerseits durch Aufwand für die Verarbeitung, Speicherung und Dokumentation von Daten und andererseits durch Zeitersparnis bei der konkreten Durchführung der jeweiligen Maßnahme.

Die Befugnis zur automatisierten Datenverarbeitung von an öffentlichen Orten durch Videoüberwachung erhobenen personenbezogenen Daten (§ 57a SächsPVDG-E) führt zu einmaligem Sachaufwand für die entsprechende technische Ausstattung der Polizeidirektionen in Höhe von 750.000 Euro. Hinzu kommt einmaliger Personal- und Sachaufwand für die Schulung der Bediensteten für die Bedienung der Analysesoftware in nicht quantifizierter Höhe. Hierbei ist von einem Umfang von 4 Arbeitsstunden pro Neu-/Erstanwender auszugehen. Der jährliche Sachaufwand im Zusammenhang mit der technischen Ausstattung beläuft sich auf 200.000 Euro. Es entsteht zudem nicht quantifizierter Personal- und Sachaufwand für die Durchführung von Analysen. Ab 2028 ist mit einem anwachsenden Fallaufkommen im mittleren einstelligen Bereich pro Jahr zu rechnen, wobei umfangreiche Analysen mehrere Stunden dauern und im Falle einer stationären Videoüberwachung gar mehrere Arbeitstage über einen Zeitraum von drei bis sechs Monaten in Anspruch nehmen können. Analysen zur Videoüberwachung auf Grundlage von § 57 Absatz 2 SächsPVDG-E können hingegen nur wenige Stunden dauern. Weiterer jährlicher Personal- und Sachaufwand in nicht quantifizierter Höhe entsteht durch Zentralstellenaufgaben wie Wartung und Support. Hier wird mit einem Personaleinsatz von zwei Polizeivollzugsbediensteten pro Dienststelle und fünf

Polizeivollzugsbediensteten im Polizeiverwaltungsamt bzw. Landeskriminalamt ausgegangen, wobei zur erforderlichen Anzahl an Stunden keine Angaben vorliegen.

Die anlassbezogene automatisierte Kennzeichenerkennung (§ 58 SächsPVDG-E) wird um die Möglichkeit des verdeckten Einsatzes erweitert. Hierfür fällt einmaliger Sachaufwand in Höhe von 150.000 Euro zur Beschaffung der entsprechenden Technik an. Zudem nimmt der Sächsische Normenkontrollrat einen jährlichen Sachaufwand in Höhe von 130.000 Euro für den Betrieb der stationären Anlagen an (für die Jahre 2026 und 2027 350.000 Euro + für das Jahr 2028 45.000 Euro / 3 Jahre). Der im Zusammenhang mit der neuen Befugnis anfallende, nicht quantifizierte jährliche Personal- und Sachaufwand wird durch nicht quantifizierte Einsparungen im Zusammenhang mit dem Einsatz mobiler Anlagen kompensiert.

Durch den Wegfall von § 59 SächsPVDG kommt es zur nicht quantifizierten Reduzierung von Personal- und Sachaufwand.

Soweit nunmehr nach § 60 Absatz 1 SächsPVDG-E eine Erweiterung um die Ausschreibung zur Ermittlungsanfrage möglich ist, entstehen auf Grundlage der Angaben zum Gesetzesvorhaben des Bundes bei 50 Anfragen und drei Arbeitsstunden eines Beamten der LG 2.1 pro Ausschreibung ein jährlicher Personalaufwand in Höhe von 8.924 Euro (50 Fälle x 3 Stunden x 59,49 Euro Personalkostensatz je Arbeitsstunde LG/E 2.1) und ein jährlicher Sachaufwand in Höhe von 1.181 Euro (50 Fälle x 3 Stunden x 7,87 Euro Sachkosten). Zugleich wird jedoch auch jährlicher Personal- und Sachaufwand in nicht quantifizierter Höhe eingespart, da andere polizeiliche Maßnahmen entbehrlich werden.

Hinsichtlich der Ausweitung des Einsatzes der elektronischen Aufenthaltsüberwachung auf Hochrisikofälle von häuslicher Gewalt („elektronische Fußfessel“, § 61 Absatz 1 Nummer 1 SächsPVDG-E) ist mit nicht quantifiziertem, erheblichen jährlichem Personal- und Sachaufwand zu rechnen. Das SMI rechnet mit fünf Anwendungsfällen pro Jahr. Sofern die länderübergreifende Verbundlösung zur Datenvereinbarung fortgesetzt werden kann, entsteht für die Erstanlegung der Fußfessel, also die Zurverfügungstellung der Ausrüstung, ein jährlicher Sachaufwand in Höhe von 25.000 Euro (5.000 Euro x 5 Fälle). Der weitere jährliche Sachaufwand (z. B. für einen etwaigen Gerätetausch, Wartung) beläuft sich schätzungsweise auf 25.000 Euro.

Die Befugnis zur anlassbezogenen automatisierten Datenanalyse (§ 62a SächsPVDG-E) zieht jährlichen Sachaufwand in Höhe von 2,5 Mio. Euro nach sich für die Bereitstellung entsprechender Software, sofern die Möglichkeit der länderübergreifenden Vernetzung besteht. Personalaufwand entsteht in nicht quantifizierter Höhe aufgrund der Prüfungs- und Begründungs-pflichten in Absatz 3 Satz 6, Absatz 5 Satz 3 und Absatz 6 Satz 2, wobei pro Anwendungsfall für diese Pflichten mit vier Stunden durch einen Bediensteten der LG/E 2.1 zu rechnen ist. Das SMI geht von schätzungsweise 100 Maßnahmen pro Jahr aus. Insofern entstehen ein jährlicher Personalaufwand in Höhe von 23.796 Euro (100 Fälle x 4 Stunden x 59,49 Euro Personalkostensatz je Arbeitsstunde LG/E 2.1) und ein jährlicher Sachaufwand in Höhe von 3.148 Euro (100 Fälle x 4 Stunden x 7,87 Euro Sachkosten). Zugleich ist jedoch mit einer nicht quantifizierten jährlichen Reduzierung des Personalaufwandes zu rechnen, da durch die automatisierte Datenanalyse gegenüber der konventionellen Datenanalyse weniger Personalressourcen gebunden werden. Insbesondere entfallen zeitintensive manuelle Arbeitsschritte, sodass mitunter wochenlange Auswertungen vermieden werden können. Es fällt zudem einmaliger Personal- und Sachaufwand für entsprechende Schulungen an. Ausgehend von geschätzten drei Schultagen und fünf zu schulenden Analysten pro Dienststellen werden 30 Analysten der LG 2.1 in 720 Stunden ausgebildet. Dadurch entstehen einmaliger Personalaufwand in Höhe von 42.833 Euro (3 Tage x 8 Stunden x 30 Personen x 59,49 Euro Personalkostensatz je Arbeitsstunde LG/E 2.1) und einmaliger Sachaufwand in Höhe von 5.666 Euro (24 Stunden x 30 Personen x 7,87 Euro Sachkosten).

Die Befugnis zum anlassbezogenen nachträglichen Abgleich mit öffentlich zugänglichen Daten aus dem Internet (§ 62b SächsPVDG-E) führt für die Beschaffung der entsprechenden Software sowie weiterer Lizenzen (Zusatzmodule) schätzungsweise zu einem jährlichen Sachaufwand in Höhe von 210.000 Euro. Zudem entsteht ein einmaliger Sachaufwand in Höhe von 15.000 Euro für die Beschaffung der erforderlichen Monitore. Pro Analyse entsteht in einfachgelagerten Sachverhalten Arbeitsaufwand für einen Bediensteten der LG/E 2.1 von einem Arbeitstag, mithin 8 Stunden, bei geschätzten 50 Fällen jährlich ab dem zweiten Jahr der Verwendung. Mithin ergeben sich jährlicher Personalaufwand in Höhe von 23.796 Euro (8 Stunden x 50 Fälle x 59,49 Euro Personalkostensatz je Arbeitsstunde LG/E 2.1) und jährlicher Sachaufwand in Höhe von 3.148 Euro (8 Stunden x 50 Fälle x 7,87 Euro Sachkosten je Arbeitsstunde).

Hinsichtlich der Befugnisserweiterung zur Quellen-Telekommunikationsüberwachung („Quellen-TKÜ“, § 66 Absatz 2 SächsPVDG-E), welche zunächst bis 31. Dezember 2031 befristet ist, entstehen einmaliger Personal- und Sachaufwand. Das SMI geht von 14 zu überwachenden Anschlüssen jährlich aus. Für die Überwachung eines Anschlusses können durchschnittlich 76,5 Arbeitsstunden für einen Polizeivollzugsbediensteten der LG/E 2.1 veranschlagt werden. Insgesamt entstehen für die Quellen-Telekommunikationsüberwachung einmaliger Personalaufwand in Höhe von 318.569 Euro (14 Telefonanschlüsse x 76,5 Arbeitsstunden x 59,49 Euro Personalkostensatz je Arbeitsstunde LG/E 2.1 x 5 Jahre) und einmaliger Sachaufwand in Höhe von 147.144 Euro [(5.355 Stunden x 7,87 Euro Sachkosten) + (14 Anschlüsse x 1.500 Euro Providerkosten x 5 Jahre)]. Soweit Übersetzungen erforderlich sind, kommt Sachaufwand in Höhe von 65 Euro pro Stunde hinzu. Für das digitale Aufspielen der Software werden im Vergleich mit bisherigen strafrechtlichen Ermittlungsverfahren im Durchschnitt drei Stunden pro Endgerät geschätzt. Existiert pro Anschluss ein Endgerät, ergeben sich bei 14 Anschlüssen ein einmaliger Personalaufwand in Höhe von 12.493 Euro (14 Telefonanschlüsse x 3 Stunden x 59,49 Euro Personalkostensatz je Arbeitsstunde LG/E 2.1 x 5 Jahre) und einmaliger Sachaufwand in Höhe von 1.653 Euro (42 Stunden x 7,87 Euro Sachkosten x 5 Jahre). Im Falle des Aufspielens per Hardware ist der Personalaufwand erheblich länger.

Nach § 70 Absatz 3 SächsPVDG-E bedürfen Maßnahmen nach § 70 Absatz 2 SächsPVDG-E keiner richterlichen Anordnung mehr. In diesem Zusammenhang kommt es zu einer nicht quantifizierten Verringerung des jährlichen Personal- und Sachaufwandes.

Soweit eine konkrete Befugnis zum Einsatz von unbemannten Luftfahrtsystemen („Drohnen“, § 71 SächsPVDG-E) geschaffen wird, zieht diese jedenfalls keinen Erfüllungsaufwand nach sich, da derartige Maßnahmen bisher bereits aufgrund der Generalklausel ergriffen wurden. Die Anschaffung weiterer Technik bzw. der Austausch solcher hängt nicht kausal mit der nunmehr konkreten Normierung der Befugnis zusammen.

Aus den §§ 74, 75 SächsPVDG-E ergeben sich neue Benachrichtigungs- und Protokollierungspflichten, die schätzungsweise bei Zugrundelegung von insgesamt 300 Arbeitsstunden zu einem jährlichen Personalaufwand in Höhe von 17.847 Euro

(300 Stunden x 59,49 Euro Personalkostensatz je Arbeitsstunde LG/E 2.1) und einem jährlichen Sachaufwand in Höhe von 2.361 Euro (300 Stunden x 7,87 Euro Sachkosten je Arbeitsstunde) führen.

Soweit nunmehr eine Befugnis zum Einsatz von Software zum Training von lernenden IT-Systemen (§ 79c SächsPVDG-E) besteht, entsteht einmaliger und jährlicher Sachaufwand in nicht quantifizierter Höhe (schätzungsweise in Höhe von mehreren Millionen Euro) für die Anschaffung/Entwicklung und den Betrieb der entsprechenden Software sowie Server. Hinzu kommen Schulungskosten in nicht quantifizierter Höhe. Es entsteht zudem einerseits jährlicher Personal- und Sachaufwand in nicht quantifizierter Höhe für die Umsetzung der neuen Befugnis, wobei andererseits jährlicher Personal- und Sachaufwand in nicht quantifizierter Höhe eingespart wird, da bisherige Tätigkeiten wegfallen.

Die Datenübermittlung an Opferberatungsstellen (§ 84 Absatz 3 Nummer 5 SächsPVDG) führt zu geschätzt 100 Datenübermittlungen pro Jahr und einem Zeiteinsatz pro Datenübermittlungsvorgang von maximal 15 Minuten. Insofern entstehen ein jährlicher Personalaufwand in Höhe von 1.487 Euro (100 x 15 Minuten / 60 Minuten x 59,49 Euro Personalkostensatz je Arbeitsstunde LG/E 2.1) und ein jährlicher Sachaufwand in Höhe von 197 Euro (25 Stunden x 7,87 Euro Sachkosten je Arbeitsstunde).

Für die Befugniserweiterung zur Erhebung von den Notruf 110 begleitenden personenbezogenen Daten einschließlich Standortdaten eines Mobilfunkendgerätes (§ 86 Absatz 1 SächsPVDG-E) bedarf es einer Anbindung an die sogenannte Advanced Mobile Location Technologie; deren bundesweiter Dauerbetrieb verursacht jährlichen Sachaufwand in Höhe von 75.000 Euro.

Die Änderung der Bezeichnung des „Polizeiverwaltungsamtes“ in „Polizeipräsidium für Service und IT“ ist mit einem einmaligen Sachaufwand in Höhe von 20.500 Euro verbunden. Es entsteht zudem einmaliger Personalaufwand durch die Änderung von Vorlagen, Briefköpfen, Signaturen etc. in Höhe von 875 Euro (35 Stunden x 25 Euro brutto durch Mitarbeiter in der E9).

Die externe Evaluation der neu geschaffenen Befugnisnormen (§§ 21 Absatz 6, 40 Absatz 5, 57 Absatz 11, 58 Absatz 6, 61 Absatz 7 und 66 Absatz 6 SächsPVDG-E) zieht im Mittelwert einmaligen Sachaufwand in Höhe von 240.000 Euro nach sich.

Zudem ergeben sich nicht quantifizierter Personal- und Sachaufwand im Zusammenhang mit der Durchführung von Ausschreibungen bzw. Vergaben zur technischen Ausstattung. Darüber hinaus entstehen Personal- und Sachaufwand in nicht quantifizierter Höhe im Hinblick auf das Sich-vertraut-Machen der mit dem neuen SächsPVDG befassten Personen.

Die neuen und ergänzten Befugnisse der Sächsischen Datenschutz- und Transparenzbeauftragten führen zu einem geschätzten zusätzlichen jährlichen Zeitaufwand in Höhe von 565 Stunden. Hierdurch ergeben sich jährlicher Personalaufwand in Höhe von 47.754 Euro (565 Stunden x 84,52 Euro Personalkostensatz je Arbeitsstunde LG/E 2.2) und jährlicher Sachaufwand in Höhe von 4.447 Euro (565 Stunden x 7,87 Euro Sachkosten je Arbeitsstunde).

Im Hinblick auf die Neuregelungen ist bei Verfahren mit richterlicher Anordnung (§§ 57 Absatz 8 Satz 6, § 57a Absatz 5 Satz 1, 60 Absatz 3 Satz 2, § 61 Absatz 3 Satz 1, § 62a Absatz 8 Satz 3 und 5, 62b Absatz 3 Satz 1 und 66 Absatz 4 Satz 1 SächsPVDG-E) mit Mehrbelastungen der Justiz zu rechnen. Der Personalbedarf im richterlichen Bereich erhöht sich hierdurch schätzungsweise um 0,26 AKA, mithin 422 Stunden, und im richterlichen Unterstützungsbereich um 0,53 AKA, mithin 861 Stunden. Dies bedeutet jährlichen Personalaufwand in Höhe von 76.892 Euro ([422 Stunden x 84,52 Euro Personalkostensatz je Arbeitsstunde LG/E 2.2] + [861 Stunden x 47,88 Euro Personalkostensatz je Arbeitsstunde LG/E 1.2]) sowie jährlichen Sachaufwand in Höhe von 10.097 Euro (1.283 Stunden x 7,87 Euro Sachkosten je Arbeitsstunde).

Ein nicht quantifizierter jährlicher Erfüllungsaufwand entsteht zudem durch die Erweiterung der Berichtspflichten gegenüber dem Landtag in § 107 SächsPVDG-E.

Eine Vielzahl von Befugnisnormen führt zunächst zu einmaligem nur teilweise quantifiziertem Erfüllungsaufwand für Beschaffungen von technischen Gerätschaften. Gleichzeitig entsteht für die Zukunft jährlicher nicht quantifizierter Erfüllungsaufwand, sofern Ersatzbeschaffungen erforderlich werden.

2.4.3.2. Erfüllungsaufwand der Kommunen

Die Änderungen haben keine Auswirkungen auf den Erfüllungsaufwand der kommunalen Ebene.

2.5. Weitere Wirkungen

Durch die neuen Ordnungswidrigkeitentatbestände (§ 106a SächsPVDG-E) sind bei den Bürgerinnen und Bürgern Geldbußen zu erwarten.

3. Bewertung durch den Sächsischen Normenkontrollrat

Der Sächsische Normenkontrollrat bittet um eine Anpassung der Darstellung des Erfüllungsaufwandes.

Wenngleich grundsätzliches Verständnis dafür besteht, dass einzelne Angaben aufgrund ihrer prognostischen Natur nur schwer zu ermitteln sind, äußert der Sächsische Normenkontrollrat Bedenken hinsichtlich der nicht vollständigen Quantifizierung der Auswirkungen auf den Erfüllungsaufwand mehrerer technischer Befugnisnormen.

Der Sächsische Normenkontrollrat bittet zudem um Überprüfung normierter Schriftformerfordernisse, insbesondere soweit die Kommunikation zwischen Polizei und Gericht betroffen ist.

Mit freundlichen Grüßen

gez. Munz
Vorsitzende

gez. Ludwig
Berichterstatte

Univ.-Prof. Dr. Dr. Markus Thiel

Deutsche Hochschule der Polizei

Fachgebiet III.4 – Öffentliches Recht mit Schwerpunkt Polizeirecht

An das
Sächsische Staatsministerium des Innern

01095 Dresden

Stellungnahme

Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG)

Anhörung des Referentenentwurfes

A. Gegenstand der Stellungnahme

Mit Schreiben des Sächsischen Staatsministeriums des Innern vom 6. Oktober 2025 wurde die Deutsche Hochschule der Polizei um Abgabe einer Stellungnahme im Rahmen der Anhörung des Entwurfes zur Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG) gebeten. Diese Änderungen sind als Artikel 1 Bestandteil eines breit aufgestellten Regierungsentwurfs zur Änderung polizeirechtlicher Vorschriften.

Der Unterzeichner als Leiter des Fachgebiets III.4 – Öffentliches Recht mit Schwerpunkt Polizeirecht – hat die Stellungnahme zu den öffentlich-rechtlichen, insbesondere den polizeirechtlichen Aspekten übernommen. Hinsichtlich des Begriffs der „Vorfeldstraftaten“ in § 4 Nr. 6 SächsPVDG wird auf die schriftliche Stellungnahme von Univ.-Prof. Dr. Lars Berster, Deutsche Hochschule der Polizei, verwiesen.

Die nachstehenden Ausführungen geben die persönlichen Auffassungen des Unterzeichners wieder und beschränken sich angesichts des Umfangs des Referentenentwurfs auf ausgewählte Aspekte. Dabei werden vor allem diejenigen Rechtsfragen des Sächsischen Polizeivollzugsdienstgesetzes aufgegriffen, die im Anhörungsschreiben explizit aufgeführt sind. Ergänzend wird auf einzelne weitere geplante Regelungen eingegangen.

B. Rechtliche Würdigung

I. Allgemeines

Der Entwurf des Gesetzes zur Änderung polizeirechtlicher Vorschriften sieht umfassende Änderungen im Sächsischen Polizeivollzugsdienstgesetz, im Sächsischen Polizeibehördengesetz, im Sächsischen Kontrollgesetz, im Sächsischen Gesetz zur Regelung polizeilicher Sicherheitsüberprüfungen sowie eine Reihe von Folgeänderungen in verschiedenen weiteren Gesetzen und Verordnungen vor. Ziel sind die Anpassung des Gesetzesbestand an die Direktiven der verfassungsgerichtlichen Judikatur und die Schaffung eines „modernen“ Befugniskatalogs. Aus Sicht des Unterzeichners gelingt dies mit dem Entwurf weitestgehend, wobei im Detail Anpassungen empfohlen werden können.

II. Erweiterung bzw. Wiederaufnahme des Tatbestandsmerkmals der „öffentlichen Ordnung“ in § 18 SächsPVDG

Zur Frage einer Wiederaufnahme der Schutzkomponente der „öffentlichen Ordnung“ in § 18 SächsPVDG hat der Unterzeichner im übersandten Referentenentwurf keine Hinweise gefunden. Offenbar wird erwogen, sie in die Ermächtigungsgrundlage für die Platzverweisung (§ 18 SächsPVDG) (wieder) aufzunehmen.

Die Diskussion über Nutzen, Belastungen und Herausforderungen der Kategorie der „öffentlichen Ordnung“ wird seit Jahrzehnten geführt und soll hier nicht im Detail nachgezeichnet werden. Die Einwände gegen ihre Verwendung im Gesetz reichen von missbräuchlicher Anwendung im Nationalsozialismus über eine fehlende Bestimmtheit bis hin zur praktischen Schwierigkeit der Feststellung, hinsichtlich welcher ungeschriebener Regeln für das Verhalten von Personen in der Öffentlichkeit eine überwiegende Mehrheit der Bevölkerung die Einhaltung für eine unerlässliche Voraussetzung für ein geordnetes gesellschaftliches Zusammenleben hält.

Die Kritik gegen die „öffentliche Ordnung“ ist nicht vorschnell von der Hand zu weisen. Gleichwohl kommt ihr nach Einschätzung des Unterzeichners eine nicht zu vernachlässigende Reservefunktion im Vergleich mit der öffentlichen Sicherheit zu: Nicht allen mehrheitlich unerwünschten Verhaltensweisen wird (schon) mit entsprechenden Ge- oder Verbotsnorm der objektiven Rechtsordnung begegnet, und nicht alle verletzen ohne weiteres Individualrechtsgüter. Die öffentliche Sicherheit lässt also Lücken insbesondere bei neueren „Trends“ der gesellschaftlichen Entwicklungen.

Das SächsPVDG trägt dem Rechnung, indem es an der öffentlichen Ordnung als Kategorie insgesamt festhält. Der Begriff ist in § 4 Nr. 2 definiert. Die Abwehr von Gefahren für die (öffentliche) Ordnung gehört nach § 2 Abs. 1 S. 2 SächsPVDG zu den polizeilichen Gefahrenabwehraufgaben. Auch die Generalklausel in § 12 Abs. 1 SächsPVDG nimmt sie in Bezug. Damit ist die öffentliche Ordnung im SächsPVDG als Kategorie grundsätzlich anerkannt. In der Ermächtigungsgrundlage zur Platzverweisung nach § 18 Abs. 1 SächsPVDG ist jedoch allein die Gefahr für die öffentliche Sicherheit angesprochen.

Insoweit erscheint es aus Sicht des Unterzeichners als ein durchaus gangbarer Weg, die Bestimmung in § 18 SächsPVDG insoweit „entwicklungsoffen“ zu halten und die öffentliche Ordnung wieder aufzunehmen (oder nur „zur Abwehr einer Gefahr“ zu schreiben; wegen § 4 Nr. 3 lit. a) SächsPVDG wären beide Schutzkomponenten erfasst). Eine willkürliche Anwendung ist nicht zu befürchten, weil die handelnden Polizeikräfte jeweils das Vorliegen der Gefahr für die öffentliche Ordnung zu prüfen hätten.

III. Bewertung der Regelung des § 57a SächsPVDG-E („Anwendungen zur automatisierten Verarbeitung von an öffentlichen Orten und besonders gefährdeten Einrichtungen offen erhobenen personenbezogenen Daten“)

§ 57a SächsPVDG-E enthält eine umfangreiche Bestimmungen zur Gestattung von Anwendungen zur automatisierten Verarbeitung von an öffentlichen Orten und besonders gefährdeten öffentlichen Einrichtungen offen erhobenen personenbezogenen Daten. Erlaubt werden sollen zum einen die Erkennung und Auswertung von Bewegungsmustern, die auf die Begehung einer Straftaten hindeuten, oder von Mustern bezogen auf Waffen im Sinne des § 1 Abs. 2 des Waffengesetzes, Messer und gefährliche Gegenstände.

Die Idee, bei der offenen Videoüberwachung begleitend automatisierte Systeme „laufen zu lassen“, die Bewegungs- und Gegenstandsmuster erkennen können, ist sachgerecht und wird den Anforderungen der polizeilichen Praxis gerecht. Werden solche Muster erkannt, wird die Polizei nach den Regelungen des Entwurfs zu einer unverzüglichen Prüfung verpflichtet, ob mit Straftaten von erheblicher Bedeutung (nach der Legaldefinition in § 4 Nr. 4 SächsPVDG) in absehbarer Zeit mit hinreichender Wahrscheinlichkeit gerechnet werden kann. Ist dies der Fall, werden weitere Optionen eröffnet: Zum einen die Kennzeichnung von Personen in Bildübertragungen und -aufzeichnungen zur automatisierten Nachverfolgung, zum anderen eine biometrische Echtzeit-Fernidentifizierung

anhand des Datenbestandes der polizeilichen Auskunfts- und Fahndungssysteme; letzteres indes nur, wenn und soweit eine erhebliche gegenwärtige Gefahr für Leib oder Leben einer Person vorliegt und wenn die Abwehr der Gefahr auf diese Weise unbedingt erforderlich ist. Ergänzende Ermächtigungen enthält § 57a Abs. 2 SächsPVDG-E.

Die vorgeschlagenen Regelungen erscheinen insgesamt sachgerecht und begegnen keinen grundlegenden verfassungsrechtlichen Bedenken. Die Eingriffsschwellen erscheinen als hinreichend hoch gesetzt, weil an anerkanntermaßen besonders gewichtige Rechtsgüter angeknüpft wird; die Durchführungs- und Verfahrensbestimmungen tragen den grundrechtlichen Belangen der überwachten Personen angemessen Rechnung. Eine automatisierte Mustererkennung kann – soweit ansonsten die Bildübertragung z. B. verzerrt oder „verwaschen“ wird – sogar eine vergleichsweise milde Maßnahme darstellen. Dass erst nach einer Prüfung auf das Vorliegen einer Straftat von zeitlich „naheliegenden“ Straftaten von erheblicher Bedeutung weitere Instrumente „freigeschaltet“ werden, erscheint ebenfalls als differenzierte Lösung, die die verfassungsrechtlichen Direktiven mit den polizeipraktischen Rahmenbedingungen in Einklang bringt.

IV. Bewertung der möglichen Drittbetroffenheit in § 66 Abs. 2a Nr. 4 und 5 SächsPVDG-E

§ 66 SächsPVDG-E regelt die Telekommunikationsüberwachung. In Absatz 2 ist die sog. „Quellen-Telekommunikationsüberwachung“ normiert, Absatz 2a bestimmt, gegen welche Personen sich die Überwachung und Aufzeichnung der Telekommunikation richten darf. Nr. 4 erfasst damit diejenigen Personen, deren Telekommunikationsanschluss oder Endgerät von einer nach Nr. 1 – 3 überwachbaren Person genutzt wird. Nr. 5 betrifft die sog. „Nachrichtenmittler“ im Dienst von Personen nach Nr. 1 – 3.

Zudem erlaubt Absatz 2a Satz 4 die Maßnahme auch dann, wenn Dritte unvermeidbar betroffen werden. Die in Nr. 4 und 5 genannten Personen sind allerdings keine „Dritte“ im Sinne des Satzes 4, weil sie in einem normativ konturierten Zusammenhang zu Personen nach Nr. 1 – 3 stehen und also solche unmittelbar „Adressaten“ (genauer: „Betroffene“) der Quellen-Telekommunikationsüberwachung sein können. Dass bei einer Überwachung von Nachrichtenmittlern oder „Anschlussbereitstellern“ jeweils auch unbeteiligte Dritte in die Maßnahme einbezogen werden und in ihre Telekommunikationsfreiheit nach Art. 10 Abs. 1 GG eingegriffen wird, beruht auf den tatsächlichen

Gegebenheiten und ist unvermeidlich. Namentlich im Falle der Nr. 4 kann die Anzahl der Betroffenen durchaus beachtlich sein.

Es wäre allerdings nicht plausibel, gewissermaßen von „zwei Klassen“ Drittbetroffener auszugehen: Solchen, die mit den in Nr. 1 – 3 genannten Personen kommunizieren, und solchen, die „nur“ mit den in Nr. 4 und 5 genannten Personen kommunizieren. Die grundrechtliche Belastungswirkung ist bei beiden Gruppen identisch, und die größere „Tatnähe“ der in Nr. 1 – 3 sollte nicht dazu führen, dass nur deren unbeteiligte Kommunikationspartner „mitüberwacht“ werden dürften. Vor diesem Hintergrund ist die Frage der Drittbetroffenheit bei § 66 Abs. 2a SächsPVDG-E einheitlich zu bewerten.

V. Weitere Regelungen

1. § 12a SächsPVDG-E – Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme

§ 12a SächsPVDG-E sieht in Satz 1 die Schaffung einer neuen Befugnisnorm zur Abwehr von Gefahren von Gefahren vor, die von unbemannten Fahrzeugsystemen ausgeht, die an Land, in der Luft oder zu Wasser betrieben werden („Drohnen“). Gestattet wird der Einsatz technischer Mittel gegen das System, dessen Steuerungseinheit oder Steuerungsverbindung, soweit die Abwehr der Gefahr auf andere Weise aussichtslos ist oder wesentlich erschwert wäre. Nach Satz 2 kann die Polizei zur Abwehr von Gefahren nach Satz 1 technische Mittel auch zur Erkennung einer Gefahr einsetzen.

Die vorgeschlagene Vorschrift ist weitestgehend an § 15e des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) angelehnt. Auch in Art. 29a des Polizeiaufgabengesetzes (Bayern) in der Fassung des Gesetzentwurfs der Staatsregierung zu einem Gesetz zum Schutz vor Drohnenüberflügen in Bayern (Drs. 19/8567) ist eine ähnliche Vorschrift vorgesehen. In weiteren Ländern wird ein entsprechendes Vorgehen derzeit diskutiert.

So naheliegend und wünschenswert es ist, verlässliche Rechtsgrundlagen für ein polizeiliches Vorgehen gegen Gefahren zu schaffen, die von „Drohnen“ ausgehen, hat der Unterzeichner Zweifel daran, ob sich dies nach geltender Rechtslage so umsetzen lässt. De lege lata wird der Einsatz technischer Mittel gegen Drohnen zur Gefahrenabwehr noch auf die Generalklausel gestützt werden können, jedenfalls soweit sich nicht aufgrund anderer Vorschriften die Zuständigkeit einer anderen Behörde ergibt. Eine dauerhafte

Anwendung der Generalklausel erscheint jedoch problematisch; so ist es grundsätzlich zu empfehlen, für spezifische Maßnahmen, deren Notwendigkeit man erkannt hat, auch jeweils „massgeschneiderte“ Befugnisnormen und Durchführungsbestimmungen zu schaffen.

Soweit allerdings die Einführung einer expliziten Ermächtigungsnorm durch den Landesgesetzgeber erfolgen soll, steht dem derzeit jedenfalls nach gängiger verfassungsrechtlicher Dogmatik die ausschließliche Gesetzgebungskompetenz des Bundes nach Art. 73 Abs. 1 Nr. 6 GG entgegen.

Danach hat der Bund die ausschließliche Gesetzgebung über „den Luftverkehr“. Zum „Luftverkehr“ gehört nach verbreiteter Auffassung in der Kommentarliteratur auch die „Luftpolizei“ – entweder als begriffliches Element oder aber als „Annex“-Kompetenz. Dazu wiederum wäre auch die Abwehr von Gefahren zu zählen, die von Luftfahrzeugen ausgehen. Nach § 1 Abs. 2 S. 3 LuftVG gelten auch unbemannte Fluggeräte einschließlich ihrer Kontrollstation, die nicht zu Zwecken des Sports oder der Freizeitgestaltung betrieben werden, als Luftfahrzeuge (unbemannte Luftfahrtsysteme). Auch das Bundesverfassungsgericht sieht es so:

„Die Gesetzgebungszuständigkeit für den Luftverkehr umfasst daher als Annex jedenfalls die Befugnis, Regelungen zur Abwehr solcher Gefahren zu treffen, die gerade aus dem Luftverkehr herrühren (...)“ (BVerfG, Beschl. v. 3. Juli 2012 – 2 PbvU 1/11, Rn. 18).

Das Bundesverfassungsgericht führt sodann weiter aus:

„Allerdings bedarf die Notwendigkeit des Zusammenhangs zwischen einer dem Bund zugewiesenen Regelungskompetenz für ein bestimmtes Sachgebiet und einschlägigen Regelungen zur Aufrechterhaltung der Sicherheit und Ordnung strenger Prüfung. Dies gilt erst recht, wenn die sachgebietliche Kompetenz zu den ausschließlichen Gesetzgebungskompetenzen des Bundes, insbesondere also zu den in Art. 73 GG aufgeführten, gehört. Jedenfalls für die Abwehr derjenigen spezifisch aus dem Luftverkehr herrührenden Gefahren, auf die die Regelungen des Luftsicherheitsgesetzes zielen, ist der erforderliche notwendige Zusammenhang gegeben. Denn bei dezentraler Regelungskompetenz hätten unzureichend abwehrwirksame Regelungen eines einzelnen Landes erhebliche negative Folgen für die

Sicherheit, die mit einiger Wahrscheinlichkeit nicht im Wesentlichen auf das betreffende Land beschränkt wären.“ (ebd., Rn. 19).

Nach Ansicht des Bundesverfassungsgerichts besteht mithin im Geltungsbereich des Luftsicherheitsgesetzes (LuftSiG) eine Annexkompetenz des Bundes für Regelungen zur Gewährleistung der Sicherheit und Ordnung im Luftverkehr.

Das LuftSiG wiederum gilt nach § 1 „dem Schutz vor Angriffen auf die Sicherheit des zivilen Luftverkehrs, insbesondere vor Flugzeugentführungen, Sabotageakten und terroristischen Anschlägen“. Dies könnte zu der Annahme verleiten, die vom Bundesverfassungsgericht postulierte Annexkompetenz des Bundes gelte nur in Bezug auf Angriffe auf die Sicherheit des zivilen Luftverkehrs, nicht aber dann, wenn ein Luftfahrzeug gegen „Ziele am Boden“ eingesetzt wird. Das Bundesverfassungsgericht betont aber in der genannten Entscheidung, dass sich die Kompetenz des Bundes auf alle Gefahren beziehe, die „gerade aus dem Luftverkehr herrühren“ – also nicht nur: ihm drohen. Dass dies zumindest teilweise auch Gegenstand und Schutzrichtung des LuftSiG ist, ergibt sich auch aus den Befugnissen aus § 14 LuftSiG, die dazu beitragen sollen, „vor einem Missbrauch von Luftfahrzeugen für kriminelle Zwecke“ zu schützen.

Diese Zweifel an der Gesetzgebungskompetenz der Länder für die Drohnenabwehr lassen sich schließlich auch nicht durch einen Verweis auf § 3 Abs. 5 LuftSiG ausräumen. Danach bleiben die „Aufgaben und Befugnisse der Polizeivollzugsbehörden (...) unberührt“. Diese Bestimmung kann nicht ohne weiteres als Delegation der gesetzlichen Regelungsbefugnisse an die Länder unter Abkehr von der grundgesetzlichen Kompetenzzuweisung verstanden werden, sondern dient im Wesentlichen der Abgrenzung von den Aufgaben und Zuständigkeiten der Luftsicherheitsbehörde.

Die vorstehenden knappen Erwägungen verdeutlichen die Komplexität der Thematik aus kompetenzrechtlicher Sicht. Dazu treten weiteren Überlegungen (räumliche bzw. funktionale Abgrenzung zu den Zuständigkeiten und Kompetenzen der Bundespolizei, der Bundeswehr, der Luftsicherheitsbehörden; Ausgestaltung einer Bundesauftragsverwaltung etc.). Es ist daher zu empfehlen, zur Vermeidung verfassungsgerichtlicher Streitigkeiten eine mit Bund und Ländern abgestimmte Vorgehensweise zu wählen.

Zu der in § 12a SächsPVDG-E vorgeschlagenen Bestimmung sind in der Sache darüber hinaus zwei Gesichtspunkte anzumerken: Zum einen bleiben die Voraussetzungen des Satzes 2 unklar: Die Polizei soll technische Mittel auch zur Erkennung einer Gefahr

einsetzen können, die aber nur zur Abwehr einer Gefahr i.S.v. Satz 1. Die Vorschrift suggeriert, dass eine Gefahr bereits vorliegen muss (um abgewehrt werden können); dann aber ist eine Gefahrenerkennung nicht mehr erforderlich. Entweder ist gemeint, dass der Einsatz zur Erkennung einer Gefahr im Rahmen der präventiven Gefahrenabwehraufgabe erfolgen kann. Daher wäre es vielleicht präziser, wie folgt zu formulieren:

„Zum Zwecke der Abwehr einer Gefahr im Sinne von Satz 1 kann die Polizei technische Mittel auch zur Erkennung einer Gefahr einsetzen.“

Zum anderen ist beim Einsatz technischer Mittel gegen „Drohnen“ stets darauf zu achten, dass keine Gefährdungen „am Boden“ entstehen. Es könnte folgender Satz 3 aufgenommen werden:

„Der Einsatz technischer Mittel darf nur erfolgen, wenn er keine Gefahr für Leben, Leib und Gesundheit unbeteiligter Personen oder für Sachen von bedeutendem Wert verursacht“.

2. § 19 SächsPVDG-E – Maßnahmen zum Schutz vor häuslicher Gewalt und sonstigen Nachstellungen

Eine umfassende Neugestaltung soll nach dem Referentenentwurf die Vorschrift in § 19 SächsPVDG erhalten. Dabei erscheint es zunächst als sachgerecht, die verschiedenen denkbaren Maßnahmen im Themenkomplex häuslicher Gewalt bzw. von Nachstellungen in einer Norm zu „bündeln“.

Dass die Eingriffsschwelle für alle Maßnahmen auf eine konkrete (einfache) Gefahr abgesenkt wird und eine gegenwärtige Gefahr (also: eine besondere zeitliche Qualität der Gefahrenlage) nicht (mehr) erforderlich sein soll, trägt den praktischen Schwierigkeiten bei der Feststellung einer gegenwärtigen Gefahr Rechnung: Sind Polizeikräfte vor Ort und drohen entsprechende Maßnahmen, ist es nicht selten, dass die akute Konfliktsituation beendet ist. Zur nordrhein-westfälischen Vorschrift zu Wohnungsverweisung und Rückkehrverbot bei häuslicher Gewalt in § 34a PolG NRW hat die Rechtsprechung entschieden, dass ein „Erstübergriff“ für eine Wohnungsverweisung und ein Rückkehrverbot (auch) aufgrund des Erfordernisses einer gegenwärtigen Gefahr nicht ausreicht.

Vor diesem Hintergrund ist die Orientierung an einer konkreten Gefahr vor allem mit Blick auf den Schutz gefährdeter Personen sachgerecht. Verfassungsrechtliche Bedenken

gegen diese „Absenkung“ bestehen aus Sicht des Unterzeichners nicht, zumal die geschützten Rechtsgüter (Leben, Leib, Freiheit oder sexuelle Selbstbestimmung) sehr hochrangig sind und die über die Maßnahmen entscheidenden Polizeikräfte ohnehin eine Verhältnismäßigkeitsprüfung unter Abwägung der sich gegenüberstehenden Interessen anzustellen haben.

Die in § 19 Abs. 1 S. 2 ff. SächsPVDG-E enthaltenen Regelungen zur Befristung der Anordnungen erscheinen insgesamt sachgerecht. Zu berücksichtigen ist allerdings, dass die in Abs. 1 S. 1 Nr. 1, Nr. 2 lit. a) – d) SächsPVDG-E aufgeführten Maßnahmen von unterschiedlicher Eingriffsintensität sind. Insbesondere Wohnungsverweisung und Rückkehrverbot entfalten eine erhebliche Belastungswirkung (unabhängig von der Frage, ob man die Grundrechte aus Art. 13 GG und/oder Art. 14 GG für betroffen hält). Dem trägt allerdings die Möglichkeit Rechnung, dass die Polizei im Einzelfall – nach pflichtgemäßem Ermessen unter Beachtung des Verhältnismäßigkeitsgrundsatzes – eine kürzere Frist festlegen kann. Damit kann sie den Besonderheiten der jeweiligen Fallkonstellation gerecht werden.

3. § 64 SächsPVDG – Einsatz einer V-Person, Verdeckte Ermittlerin und Verdeckter Ermittler

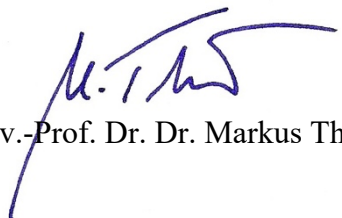
Die vorgeschlagene Neufassung des § 64 SächsPVDG-E trägt den verfassungsgerichtlich formulierten Anforderungen an den Einsatz von Vertrauenspersonen und verdeckten Ermittlerinnen bzw. -ermittlern Rechnung. Von besonderer Bedeutung sind dabei namentlich die Vorschriften zum Schutz des Kernbereichs privater Lebensgestaltung in Absatz 4. Diese erscheinen als differenziert und berücksichtigen auch die Rolle und den Pflichtenbestand der polizeilichen Kontaktpersonen.

Nicht angesprochen ist in der Norm die Problematik, dass sich namentlich beim Einsatz verdeckter Ermittler eine Verletzung des Kernbereichs bereits aus dem Aufbau einer persönlichen Vertrauensbeziehung und deren Ausnutzung unter Täuschung ergeben kann (BVerfG, Beschl. v. 9. Dezember 2022 – 1 BvR 1345/21, Rn. 103 ff.). Allerdings stellt sich ohnehin die Frage, wie diese verfassungsgerichtliche Erkenntnis normativ umgesetzt werden sollte. In § 47 Abs. 2 S. 4 des Bremischen Polizeigesetzes ist normiert: „Eine verdeckt ermittelnde Person darf unter der Legende keine sexuellen Handlungen vornehmen oder an sich vornehmen lassen und keine Liebesverhältnisse eingehen“. Auf eine

vergleichbare Bestimmung, die als „Fremdkörper“ innerhalb des Polizeirechts erschiene, verzichtet der vorliegende Entwurf richtigerweise.

Ausdrücklich zu begrüßen sind die Regelungen in Absatz 5. Ausgeschlossen werden als Vertrauenspersonen Minderjährige und Betreute sowie nach §§ 53, 53a StPO Zeugnisverweigerungsberechtigte. Es sollte erwogen werden, den Kreis der ausgeschlossenen Personen noch zu erweitern. Im Gesetzentwurf der Bundesregierung zu einem Gesetz zur Regelung des Einsatzes von Verdeckten Ermittlern und Vertrauenspersonen sowie zur Tatprovokation vom 8. Mai 2024 (BT-Drs. 20/11312) sind in der vorgeschlagenen neuen Bestimmung zu Vertrauenspersonen in § 110b Abs. 6 StPO-E weitere Personengruppen benannt, die nicht eingesetzt werden dürfen oder sollen. Trotz der Bezüge zum repressiven Handlungsfeld und den entsprechenden Besonderheiten (z. B. Ausschluss von Teilnehmerinnen und Teilnehmern an Aussteigerprogrammen) wäre etwa zu erwägen, ob nicht auch der Einsatz solcher Personen ausgeschlossen werden sollte, bei denen die Geld- oder Sachzuwendungen für den Einsatz auf Dauer ihre wirtschaftliche Lebensgrundlage darstellen, deren kumulative aktive Einsatzzeit als Vertrauensperson insgesamt mehr als zehn Jahre beträgt usw.

Münster, den 14. November 2025



(Univ.-Prof. Dr. Dr. Markus Thiel)

Stellungnahme der Jusos Sachsen zum Entwurf des Gesetzes zur Änderung polizeirechtlicher Vorschriften

Demokratie braucht Vertrauen, nicht Misstrauensarchitekturen

Die Jusos Sachsen begrüßen, dass nach dem Urteil des Sächsischen Verfassungsgerichtshofs vom 25. Januar 2024 (Vf. 91-II-19) eine Überarbeitung des Polizeirechts erfolgt. Das Urteil war ein deutlicher Weckruf: Teile des bisherigen Polizeiaufgabengesetzes sind verfassungswidrig, weil sie Freiheitsrechte aushöhlen, Eingriffsschwellen verwischen und Kontrolle erschweren.

Wir halten fest: Der vorliegende Entwurf geht über die gerichtliche Korrektur weit hinaus. Er schafft neue Befugnisse, weitet polizeiliche Eingriffskompetenzen aus und verschiebt den Maßstab von Notwendigkeit zu Machbarkeit.

Das Innenministerium nutzt den Anpassungsauftrag, um ein Polizeigesetz vorzulegen, das technisch modernisiert, aber rechtsstaatlich zurückbaut. Damit steht nicht nur das Verhältnis von Freiheit und Sicherheit, sondern das Grundvertrauen zwischen Staat und Gesellschaft zur Debatte.

Erweiterung ohne Legitimation, Prävention ohne Kontrolle

2.1 Unzureichende Umsetzung des Verfassungsgerichtsurteils

Das Urteil verlangte eng definierte Voraussetzungen für Eingriffe: eine „konkretisierte Gefahr“ und ein richterlich überprüfbares Verfahren. Der Gesetzentwurf bleibt hier vage. Es fehlt eine Definition der „konkretisierten Gefahr“; zugleich werden neue Eingriffe geschaffen, die auf Vorfeldannahmen beruhen. Das bedeutet: Der Staat will wieder in Bereiche eingreifen, in denen noch keine konkrete Gefahr besteht – exakt das, was der Verfassungsgerichtshof verboten hat.

Auch die Benachrichtigungspflichten (§ 74) bleiben schwach. Wer überwacht wird, erfährt es in vielen Fällen nicht. Ohne Wissen gibt es keinen Rechtsschutz – ohne Rechtsschutz keine Demokratie im Alltag.

Neue Befugnisse ohne klaren Bedarf

Der Entwurf enthält eine Vielzahl an neuen Befugnissen, die weder durch das Verfassungsgerichtshofsurteil noch durch empirische Sicherheitsanalysen begründet sind. Diese Maßnahmen stehen nicht im Koalitionsvertrag. Das an sich

ist kein Rechtsverstoß. Aber sie unterlaufen das im Vertrag verankerte politische Leitbild „eine[r] vernünftige[n] Balance zwischen Freiheit und Sicherheit“.

§ 12a – Einsatz und Abwehr von Drohnen

§ 12a erlaubt den Einsatz polizeilicher Drohnen sowie elektronische Gegenmaßnahmen gegen unbemannte Systeme. Damit wird der Polizei eine neue Eingriffsbefugnis im Luftraum eröffnet, ohne klare technische und rechtliche Begrenzung.

Die Norm ist zu weit und unbestimmt: Sie definiert weder den zulässigen Zweck der Datenerhebung noch Grenzen gegenüber zivilen oder militärischen Luftraumnutzungen. Dadurch entsteht ein neuer, kaum kontrollierbarer Überwachungsbereich, in dem Eingriffe in Kommunikationsnetze oder Privatsphäre Dritter nicht ausgeschlossen sind.

§ 40 – Taser für den gesamten Polizeivollzugsdienst

Hier wird ein potenziell tödliches Zwangsmittel in den regulären Streifendienst eingeführt, ohne dass eine belastbare wissenschaftliche Bewertung zu Wirkung, Risiken und Alternativen vorliegt.

Der Taser gilt häufig als „deeskalierendes“ Mittel, führt in der Praxis aber nachweislich zu einer niedrigeren Hemmschwelle für Waffeneinsatz und erhöht das Risiko schwerer Verletzungen – insbesondere bei gesundheitlich vorbelasteten Personen.

§ 57 Abs. 9 – Präventive Videoüberwachung im Straßenverkehr

Hier wird eine anlasslose, präventive Verkehrsüberwachung gesetzlich ermöglicht. Die Regelung ist unverhältnismäßig und grundrechtlich bedenklich: Sie erlaubt Eingriffe in das Recht auf informationelle Selbstbestimmung ohne konkreten Verdacht, auf Basis unbestimmter „tatsächlicher Anhaltspunkte“. Damit droht eine Dauerüberwachung des fließenden Verkehrs, die über den verfassungsrechtlich zulässigen Rahmen hinausgeht

§§ 57a & 62b – „Intelligente“ Videoüberwachung & biometrische Echtzeit-Identifikation

Mit §§ 57a und 62b würde die Polizei in Sachsen erstmals Befugnisse zur Gesichtserkennung, Musteranalyse und automatisierten biometrischen Auswertung erhalten. Das bedeutet faktisch die Einführung von Echtzeit-Biometrie im öffentlichen Raum.

Solche Systeme greifen tief in die informationelle Selbstbestimmung und Bewegungsfreiheit ein. Sie erzeugen unweigerlich Massenaufzeichnungen Unbeteiligter, ermöglichen lückenlose Bewegungsprofile und wirken abschreckend auf demokratische Teilhabe, insbesondere auf Versammlungen. Damit sind sie mit Art. 8 EU-Grundrechtecharta und Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG unvereinbar.

Der Gesetzentwurf erkennt, dass die EU-KI-Verordnung biometrische Echtzeitüberwachung als „Hochrisiko-Technologie“ einstuft und deren Einsatz nur unter extrem engen Voraussetzungen zulässt. Sachsen würde mit dieser Regelung einen europaweiten Sicherheitsausreißer schaffen.

§ 58 – Erweiterung der automatisierten Kennzeichenerfassung

Die vorgesehene Ausweitung der automatisierten Kennzeichenerfassung auf „grenzüberschreitende Kriminalität“ bedeutet eine massive Zweckausdehnung. Dadurch wird ein Instrument geschaffen, das nicht mehr punktuell, sondern dauerhaft Bewegungsdaten Unbeteiligter erfasst.

Diese Form anlassloser Datensammlung steht im Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts, das solche Systeme nur bei konkret abgrenzbaren Gefahrenlagen zulässt. Die vorgesehene Norm bleibt jedoch unbestimmt und öffnet die Tür zu einer flächendeckenden Verkehrsüberwachung.

§ 62a – Automatisierte Datenanalyse

§ 62a schafft die Grundlage für automatisierte Auswertungen polizeilicher Datenbestände – faktisch eine Öffnung für Predictive Policing. Solche Systeme erzeugen algorithmische Risikoprognosen über Personen oder Orte, ohne dass eine konkrete Gefahr oder Straftat vorliegt.

Damit wird die Logik der Gefahrenabwehr umgekehrt: aus Daten werden Verdachtsmomente konstruiert. Das birgt hohe Risiken diskriminierender Verzerrungen und entzieht sich öffentlicher Kontrolle. Eine rechtliche, technische oder wissenschaftliche Grundlage für die Wirksamkeit solcher Analysen fehlt.

§ 79c – Training und Test lernender Systeme

Hier wird der Einsatz und das Training „lernender IT-Systeme“ auf polizeilichen Datenbeständen erlaubt, ohne Beschränkung auf synthetische oder anonymisierte Daten. Damit könnten reale personenbezogene Informationen zu Trainingszwecken genutzt werden – ein klarer Bruch mit dem Grundsatz der Zweckbindung und des Datenschutzrechts.

Solche Verfahren schaffen nicht Transparenz, sondern Blackbox-Entscheidungen: Weder die Datengrundlage noch die Lernlogik der Systeme wäre überprüfbar. Damit verliert staatliches Handeln seine Nachvollziehbarkeit – ein Kernproblem aus rechtsstaatlicher Sicht.

§ 84 Abs. 2 – Datenübermittlung an andere Behörden

Die geplante Erweiterung der Datenübermittlung erlaubt, polizeiliche Informationen auch an Behörden ohne Gefahrenabwehraufgabe weiterzugeben. Damit wird ein gefährlicher Präzedenzfall geschaffen: Daten, die unter hohem Grundrechtseingriff erhoben wurden, könnten künftig behördenübergreifend zirkulieren, ohne dass Betroffene es erfahren oder ein Gericht dies kontrolliert.

Das ist ein Tabubruch im Datenschutzrecht. Die Zweckbindung wird faktisch aufgehoben – und aus gezielter Gefahrenabwehr wird ein undurchsichtiges Datennetz staatlicher Stellen. So entsteht Machtkonzentration statt rechtsstaatlicher Kontrolle.

§ 88 – Zuverlässigkeitsüberprüfungen bei Veranstaltungen

Die Norm ermöglicht Sicherheitsüberprüfungen von Personen im Umfeld bestimmter Veranstaltungen, auch bei ausländischem Wohnsitz. Diese Regelung ist völlig unverhältnismäßig und öffnet die Tür zu präventiven Gesinnungs- und Herkunftsprüfungen, die mit demokratischen Grundprinzipien unvereinbar sind. Sie ersetzt konkrete Gefahrenanalysen durch pauschales Misstrauen – und riskiert diskriminierende Praxis gegenüber Menschen ohne deutschen Pass oder mit Migrationsgeschichte. Eine derart weit gefasste Überprüfungskompetenz ist weder erforderlich noch verfassungsrechtlich haltbar.

Sicherheitspolitik am Scheideweg

Der Entwurf verschiebt Sicherheitspolitik: Von einer Gefahrenabwehr, die im Ausnahmefall eingreift, hin zu einer präventiven Dauerlogik, die technisch alles absichert, was denkbar ist. Diese Form der Sicherheitspolitik ist nicht zukunftsfähig. Sie ist teuer, intransparent und rechtlich anfällig – und sie erzeugt ein Misstrauensverhältnis zwischen Bürger*innen und Staat. Sicherheit entsteht durch Rechtsstaatlichkeit, Vertrauen und soziale Stabilität, nicht durch permanente Datenerhebung. Wer Freiheit aus Angst aufgibt, verliert am Ende beides – Sicherheit und Demokratie.

Unsere Forderungen

- Legaldefinition der „konkretisierten Gefahr“ im allgemeinen Teil des PVDG.
- Streichung oder deutliche Einschränkung der §§ 12a, 40, 57 Abs. 9, 57a, 58, 62a, 62b, 79c, 84 Abs. 2 und 88.
- Richterliche Genehmigungspflicht und Benachrichtigungspflicht für alle verdeckten Maßnahmen.
- Verbot biometrischer Echtzeit-Überwachung und algorithmischer Datenanalyse im Polizeirecht.
- Verbindliche Lösch- und Berichtspflichten für alle Datenverarbeitungen.
- Regelmäßige Evaluation der Eingriffsbefugnisse mit Beteiligung der Zivilgesellschaft.

Ein modernes Polizeigesetz ist kein Überwachungsgesetz

Der vorliegende Entwurf nutzt den Auftrag des Verfassungsgerichtshofs nicht für eine Stärkung des Rechtsstaats, sondern für die Ausweitung polizeilicher Kontrollinstrumente. Das ist eine vertane Chance für eine demokratische Sicherheitspolitik. Wir fordern eine echte Reform: Ein Polizeigesetz, das klar begrenzt, transparent kontrolliert und gesellschaftlich legitimiert ist. Sachsen braucht eine Polizei mit starken Befugnissen im Ernstfall. Sachsen braucht aber keine Polizei, die dauerhaft Daten über seine Bevölkerung sammelt, um vorbereitet zu sein, falls etwas passieren könnte.

Ein freiheitlicher Staat beweist seine Stärke nicht durch allgegenwärtige Kontrolle, sondern durch das Vertrauen, das er seinen Bürger*innen entgegenbringt.

Mit freundlichen Grüßen
Landesvorstand der Jusos in der SPD Sachsen

(Bezug: Urteil des Sächsischen Verfassungsgerichtshofs vom 25. Januar 2024;
Synopsis des Gesetzentwurfs)

SÄCHSISCHE STAATSKANZLEI
01095 Dresden

SMI Referat Polizeirecht
Anhoerung.SaechsPVDG@smi.sachsen.de

Ihr Ansprechpartner
Caterina Lotze-Kaufhold

Durchwahl
Telefon +49 351 564-13080
Telefax +49 351 564-12269

caterina.lotze-kaufhold@
sk.sachsen.de*

Ihr Zeichen

Ihre Nachricht vom

Geschäftszeichen
(bitte bei Antwort angeben)

Dresden,
7. November 2025

Stellungnahme

Die Unabhängige zentrale Vertrauens- und Beschwerdestelle für die Polizei (UVBP) begrüßt grundsätzlich die Fortentwicklung polizeilicher Befugnisse, die sich an den technischen Entwicklungen und aktuellen Gefahrenlagen orientiert.

Die UVBP hat unter anderem die Aufgabe, Beschwerden von Bürgerinnen und Bürgern gegen Mitarbeiterinnen und Mitarbeiter der Landespolizei zu prüfen. Aus diesem Grund nehmen wir vornehmlich zu den im vorgelegten Gesetzentwurf normierten Regelungen Stellung, die für uns aufgrund der bisher gemachten Erfahrungen unmittelbar Auswirkungen auf die Arbeit der UVBP haben könnten.

1. Bedenken bestehen gegen die Verfassungsmäßigkeit des Bodycam-Einsatzes in Wohnungen.

Mit § 57 Abs. 4 bis 8 SächsPVDG-E wird der Einsatz von Bodycams auf den Bereich von Wohnungen erweitert. Dies stellt unbestritten einen Eingriff in das Grundrecht der Unverletzlichkeit der Wohnung gem. Art. 13 GG dar. Art. 13 GG selbst wie auch das BVerfG in korrespondierender weiter Auslegung des Grundrechts stellen hohe Anforderungen an Eingriffe in die Unverletzlichkeit der Wohnung. Rechtfertigungsmöglichkeiten für den präventivpolizeilichen Einsatz von Bodycams bieten Art. 13 Abs. 4 und 5 GG. Art. 13 Abs. 4 GG erscheint als Schranke vor allem praxisuntauglich, da der Einsatz von Bodycams in Wohnungen in der polizeilichen Praxis meistens nicht vorherseh- und planbar sein dürfte und die vorherige Einholung der erforderlichen richterlichen Anordnung praxisfern ist. Insofern kann eine Vereinbarkeit des präventivpolizeilichen Einsatzes von Bodycams in Wohnungen nur noch über Art. 13 Abs. 5 GG erreicht werden. Der Wortlaut des Art. 13 Abs. 5 S. 1 GG verstärkt allerdings die Zweifel, ob dieser überhaupt auf den Bodycam-Einsatz übertragbar ist. Technische Mittel sind danach „ausschließlich“ zum Schutz der eingesetzten Personen vorgesehen. Der Gesetzentwurf enthält jedoch zusätzlich zur Eigensicherung der tätigen Personen (Polizeibeamten) auch die Abwehr einer dringenden Gefahr für Leib oder Leben einer dritten Person. Es ist nicht abzustreiten, dass eine Bodycam für beide Seiten sinnvoll ist, sowohl für Polizistinnen und Polizisten als auch für Bürgerinnen und Bürger.



Die Kampagne des
Freistaates Sachsen.



Hausanschrift:
Sächsische Staatskanzlei
Unabhängige zentrale
Vertrauens- und
Beschwerdestelle für die
Polizei
Archivstraße 1
01097 Dresden

www.sachsen.de

Verkehrsverbindung:
Zu erreichen mit den Straßenbahnlinien 3, 6, 7, 8, 9, 13

Für Besucher mit Behinderungen befinden sich gekennzeichnete Parkplätze am Königsufer.
Für alle Besucherparkplätze gilt: Bitte beim Pfortendienst melden.

* Der Empfang von elektronisch signierten und/oder verschlüsselten elektronischen Dokumenten ist möglich. Die öffentlichen Schlüssel der Sächsischen Staatskanzlei finden Sie unter <https://www.sachsen.de/kontakt.html>.

Sie empfinden es nicht nur deeskalierend, sie empfinden es auch als Sicherung und Sicherheit. Mecklenburg-Vorpommern, Baden-Württemberg, Nordrhein-Westfalen und Bayern haben den Aspekt mit den Wohnungen aufgenommen und schützen Dritte. Der Umstand alleine, dass auch andere Länder solche Regelungen haben, ist jedoch noch nicht Gewähr dafür, dass diese Regelung verfassungsmäßig wäre. Unserer Ansicht nach kann der Schutz Dritter auf Grundlage von Artikel 13 GG nicht verfassungsgemäß sicher geregelt werden.

Zum anderen sieht Artikel 13 Abs. 5 Satz 1 GG zwar keinen Richtervorbehalt vor, sondern verlangt nur eine Anordnung der Maßnahme durch eine gesetzlich bestimmte Stelle. Dieser Vorgabe kann durch eine Übertragung der Anordnungscompetenz auf die Einsatzleitung vor Ort Rechnung getragen werden (vgl. § 15 c II S. 2 NWPolG, § 33 IV S.3 BremPolG, § 31 Abs.2 RPPOG). Im vorliegenden Gesetzentwurf findet sich jedoch keine Regelung, wer diese Anordnung erlässt.

Insofern ist fraglich, ob überhaupt eine Ausrichtung an Art. 13 Abs. 5 GG erfolgt ist. In der Begründung des Gesetzentwurfes findet sich keine aussagekräftige Ausführung zur Beschränkung des Grundrechts nach Art. 13 GG. In der Begründung wird lediglich Art. 13 Abs. 7 GG herangezogen. Ein Rückgriff auf Art. 13 Abs. 7 GG erscheint nicht angebracht; denn Art. 13 Abs. 7 GG regelt nicht das Gleiche. Insofern ist keine Spezialität zwischen Art. 13 Abs. 7 und Abs. 4 oder 5 gegeben, sondern Abs.7 enthält schlichtweg eine Auffangnorm. Daher bestehen erhebliche Zweifel, ob die Regelung einer gerichtliche Überprüfung standhält.

2. Zahlreiche Beschwerden erreichen die UVBP aus dem Bereich der Unfallaufnahmen und polizeilichen Verkehrskontrollen. Insofern wird aus hiesiger Sicht damit gerechnet, dass durch die neue Regelung des § 57 Abs. 9 SächsPVDG-E auch die Beschwerden gegen diese Maßnahme die UVBP erreichen werden. Künftig sollen automatisiert Aufnahmen in Fahrzeuge hinein angefertigt werden dürfen, um das Benutzen elektronischer Geräte entgegen § 23 Abs. 1a StVO im öffentlichen Straßenverkehrsraum zu erkennen. Eine technische Verfahrensbeschreibung fehlt leider in der Begründung. Verstöße gegen § 23 Abs. 1a StVO stellen gemäß § 49 Abs. 1 Nr. 22 StVO eine Ordnungswidrigkeit dar. Deren Verfolgung setzt nach § 46 Abs. 1 OWiG i.V.m. § 152 Abs. 2 StPO das Vorliegen eines Anfangsverdachts voraus. Ein solcher Anfangsverdacht liegt aber im Zeitpunkt der Datenerhebung, also bei der Erfassung der Fahrzeuge noch nicht vor. Vielmehr werden zunächst alle Verkehrsteilnehmer erfasst. Die Aufgabe der in § 57 Abs. 9 Satz 1 genannten „Verhütung“ von Straftaten setzt jedoch ein präventives Tätigwerden voraus, das es gar nicht erst zu dem schädigenden Ereignis in Form der Begehung von Ordnungswidrigkeiten kommen lassen will. Die Geeignetheit der Maßnahme muss hier bezweifelt werden, da das Ziel der Verhütung von Straßenverkehrsverstößen praktisch gar nicht erreicht werden kann. Damit geht es nur um die Verfolgung von Ordnungswidrigkeiten, die nach Art. 74 Abs. 1 Nr. 2 bzw. Nr. 22 GG in die Gesetzgebungszuständigkeit des Bundes fallen. Dafür spricht der in der Gesetzesbegründung enthaltene Verweis darauf, dass als Rechtsgrundlage für eine Datenspeicherung bezüglich der mit technischem Mittel zur Bildübertragung festgestellten Verstöße der bundesrechtliche § 100h Abs. 1 Satz 1 Nr. 1 StPO in Verbindung mit § 46 Abs. 1 OWiG in Betracht kommen soll. Die Gesetzgebungskompetenz des Freistaates Sachsen ist daher zweifelhaft. Bedenken bestehen im Übrigen auch wegen der Verhältnismäßigkeit. In der Begründung zum Gesetzentwurf heißt es, dass die Ablenkung durch elektronische Geräte eine der Hauptunfallursachen bei schweren Personenschäden ist.

Hierfür werden jedoch keinerlei statistische Erhebungen angeführt, die diese Aussage untermauern. Das Statistische Bundesamt führt in seiner Unfallstatistik Verstöße gegen § 23 Abs. 1a StVO nicht als eigene Ursachenkategorie auf (<https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Verkehrsunfaelle/Tabellen/fehlverhalten-fahrzeugfuehrer.html>).

Mit freundlichen Grüßen

gez.
Caterina Lotze-Kaufhold
Leiterin UVBP



**Deutsche Hochschule
der Polizei**
Universität der Polizeien
des Bundes und der Länder

Deutsche Hochschule der Polizei · Postfach 480353 · 48165 Münster

Sächsisches Staatsministerium des Innern
01095 Dresden

Frau Peggy Frey

Department III
Kriminal- und Rechtswissen-
schaften
Fachgebiet Strafrecht, Straf-
verfahrensrecht

Prof. Dr. Lars Berster
Telefon: +49 2501 806 - 540
E-Mail: lars.berster@dhpol.de

Geschäftszeichen 36-2002/25/14

Stellungnahme zu § 4 Nr. 6 SächsPVDG-E

I. Einleitung

Mit der geplanten Einführung einer neuen Nr. 6 in § 4 SächsPVDG reagiert der Gesetzgeber auf das Urteil des SächsVerfGH vom 25. Januar 2024 (Vf. 91-II-19). Dieser hatte beanstandet, dass einzelne Befugnisnormen des Sächsischen Polizeivollzugsdienstgesetzes auf Straftatenkataloge verweisen, die auch bloße Vorbereitungshandlungen oder abstrakte Gefährdungstatbestände erfassen, und dadurch die Eingriffsschwellen für besonders grundrechtsintensive Maßnahmen zu niedrig ansetzen. Mit der Neufassung soll die Regelungstechnik angepasst und den verfassungsrechtlichen Anforderungen an die Bestimmtheit und Eingriffsintensität Rechnung getragen werden.

Die Legaldefinition in § 4 Nr. 6 SächsPVDG-E bestimmt die „Vorfeldstraftat“ als einen

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

An diese Definition knüpfen mehrere Befugnisnormen für besonders grundrechtsrelevante Standardmaßnahmen an (§§ 21 II, 57a II, 60 I, 61 I, 66 I, 62a I, 63 II, 66 IIa SächsPVDG-E), die die Zulässigkeit der Maßnahme zur Verhinderung von Vorfeldstraftaten an die zusätzliche Voraussetzung knüpfen, dass

„(...) im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen.“

Diese Formulierung spiegelt die Definition der „konkretisierten Gefahr“ durch den SächsVGH¹ und das BVerfG² wider. Gleichwohl weisen sowohl sie als auch die Umschreibung der Vorfeldstraftat einige korrekturbedürftige Unklarheiten auf.

II. Problem: Verschleifung von abstrakten Gefährdungsdelikten und pönalisierten Vorbereitungshandlungen.

Der SächsVerfGH unterscheidet in seinem Urteil durchgängig zwischen abstrakten Gefährdungsdelikten (die er unpräzise als „bloße Rechtsgutsgefährdungen“ bezeichnet) und pönalisierten Vorbereitungshandlungen und stellt klar, dass in *beiden* Fällen eine zumindest „konkretisierte Gefahr“ für das geschützte Rechtsgut hinzutreten muss, um die entsprechenden Standardmaßnahmen zu rechtfertigen. § 4 Nr. 6 SächsPVDG-E fasst beide Fälle – was an und für sich unproblematisch ist – unter dem Gattungsbegriff der „Vorfeldstraftat“ zusammen, verschleift sie dann jedoch innerhalb der Definition zu einem *einheitlichen* Phänomen, von dem überdies undeutlich bleibt, ob die „Vorbereitungshandlung“ ein eigenständiger, konstitutiver Definitionsbestandteil sein soll – also eine Begrenzungsfunktion entfaltet –, oder ob sie lediglich deskriptiv die zuvor genannten Merkmale („Handlungen im Vorfeld einer Gefährdung oder Verletzung“) zusammenfasst. Eine Entscheidung für die eine oder andere Variante wäre nicht nur semantischer Natur, sondern hätte erhebliche Auswirkungen auf den sachlichen Anwendungsbereich der korrespondierenden Befugnisnormen.

Verstünde man den Begriff der Vorbereitungshandlung als eigenständiges definitorisches Element und legte ihn – was angesichts des strafrechtlichen Kontexts zumindest nahe läge – im strafrechtlichen Sinne aus, dann wäre eine „Vorfeldstraftat“ nur in Fällen gegeben, in denen der Täter vorsätzlich eine generell gefährliche und strafbewehrte Handlung vollzieht, die *nach seinem Tatplan* in eine spätere Verwirklichung einer Rechtsgutsverletzung oder -gefährdung münden soll. Der Begriff der Vorfeldstraftat würde hierdurch stark verengt. Erfasst würden nur solche abstrakten Gefährdungsdelikte, die entweder bereits ausdrücklich Vorsatzhandlungen mit spezifischer Zielrichtung auf eine spätere Haupttat pönalisieren oder die ein Täter *in concreto* mit Blick auf eine tatplanmäßige spätere konkrete Gefährdung oder Verletzung des angegriffenen Guts verübt. Derart eng verstanden könnte die Definition demnach ihre vom SächsVerfGH geforderte und vom Gesetzgeber intendierte Begrenzungsfunktion nicht erfüllen.

¹ SächsVerfGH, Urte. v. 25. Januar 2024 (Vf. 91-II-19), C. I. 2) b) cc).

² BVerfG, Urte. v. 1.10.2024, I BvR 1160/19, Rn. 106.

Diese Bedenken bleiben auch dann bestehen, wenn man der zweiten Auslegungsmöglichkeit folgt und den Begriff der „Vorbereitungshandlungen“ nicht konstitutiv, sondern lediglich als eine paraphrasierende Umschreibung des vorangegangenen Satzteils versteht. Für ein solches Verständnis spräche der Wortlaut „... liegen können *und damit* [!] strafbewehrte Vorbereitungshandlungen darstellen“. Die Wendung „und damit“ legt nahe, dass alle strafbewehrten und typischerweise gefährlichen Handlungen im Vorfeld einer konkreten Rechtsgutsgefährdung oder Verletzung notwendig als „Vorbereitungshandlung“ einzustufen sind. Nach diesem Verständnis wären nun zwar sämtliche abstrakten Gefährdungsdelikte umfasst, außer Betracht blieben jedoch die durchaus zahlreichen strafbewehrten Vorbereitungshandlungen, die nicht zugleich auch abstrakte Gefahren für das geschützte Gut begründen.

Bsp.: Wer sich zur Vorbereitung einer geplanten Geldfälschung eine Matrize verschafft, macht sich nach § 149 StGB strafbar, ohne dass mit einem solchen Verhalten bereits typischerweise eine Gefährdung für das geschützte Gut – die Sicherheit und Funktionsfähigkeit des Geldverkehrs – verbunden wäre.

Auch in dieser Auslegung erweist sich die Definition demnach als zu eng, um die Bindung der Eingriffsbefugnis an eine zumindest „konkretisierte Gefahr“ für das angegriffene Rechtsgut in allen verfassungsrechtlich gebotenen Fällen sicherzustellen.

Eine naheliegende Lösung besteht darin, die Definition der Vorfeldstraftat stärker an die Vorgabe des SächsVerfGH anzulehnen, indem abstrakte Gefährdungsdelikte und pönalisierte Vorbereitungshandlungen definitorisch deutlich getrennt und als zwei unterschiedliche Varianten einer Vorfeldstraftat ausgewiesen werden.

Formulierungsvorschlag:

„Vorfeldstraftat: Straftatbestand, der Verhaltensweisen erfasst, die in räumlicher oder zeitlicher Hinsicht noch vor einer konkreten oder konkretisierten Gefährdung oder gar Verletzung der geschützten Individualrechtsgüter oder Kollektivrechtsgüter liegen können und vom Gesetzgeber entweder aufgrund ihrer abstrakten Gefährlichkeit oder als Vorbereitungshandlungen unter Strafe gestellt werden.“

III. Problem: Unklarheit der Schutzgüter abstrakter Gefährdungsdelikte bei Verweisung auf Vorfeldstraftaten

Den verfassungsgerichtlichen Vorgaben des des SächsVerfGH entsprechend knüpft der Entwurf bei „Vorfeldstraftaten“ besonders eingriffsintensive polizeiliche Standardmaßnahmen an das Vorliegen einer zumindest „konkretisierten Gefahr“, d.h. an „tatsächliche Anhaltspunkte für eine Gefahr für das durch die jeweilige Straftat geschützte

Rechtsgut“. Damit wird das *Schutzgut der Straftat* zum Bezugspunkt gefahrenabwehrrechtlicher Prognosen. Dieser Weg klingt plausibel und dürfte angesichts der Vorgaben des SächsVerfGH und des BVerfG aus gesetzgeberischer Sicht im Prinzip unumgänglich sein, wird jedoch bei zahlreichen abstrakten Gefährdungsdelikten nachgerade zwangsläufig zu erheblichen Bestimmtheits- und Anwendungsproblemen führen. Zu beachten ist, dass der Bundesgesetzgeber die immer umfangreichere Zahl abstrakter Gefährdungsdelikte (und pönalisierter Vorbereitungshandlungen) nicht selten mit dem Schutz „obskurer“,³ weitgehend konturloser Kollektivrechtsgüter rechtfertigt (Sicherheit und Zuverlässigkeit des bargeldlosen Zahlungsverkehrs (152a StGB), öffentlicher Friede (z.B. § 126 StGB), Vertrauen der Allgemeinheit in Märkte (§ 119 WpHG), finanzielle Interessen der Allgemeinheit (§ 370 AO) etc.).⁴ In zahlreichen weiteren Fällen herrscht heillosen Streit über die abstrakten Gefährdungsdelikten zugrunde liegenden Schutzgüter.

Vgl. hierzu exemplarisch zu § 89a StGB: Engelstädter, Leipziger Kommentar (13. Aufl.), § 89a Rn. 14: „Die Bestimmung der durch § 89a geschützten Rechtsgüter ist umstritten. Ein Teil der Literatur geht davon aus, dass die Vorschrift nur die hinter den in Absatz 1 genannten schweren Straftaten des Besonderen Teils des StGB stehenden Rechtsgüter schützen will und keine überindividuellen Rechtsgüter wie die „öffentliche Sicherheit“ oder den „öffentlichen Frieden“ erfasst. Nach der überwiegenden Ansicht erfasst die Vorschrift jedoch auch staatsschutzbezogene Rechtsgüter, wobei allerdings teilweise von einer Identität mit den durch § 129a geschützten Rechtsgütern ausgegangen wird, teilweise nur die im Tatbestand ausdrücklich erwähnten Rechtsgüter (Bestand und Sicherheit eines Staates, Verfassungsgrundsätze der Bundesrepublik Deutschland) geschützt sein sollen. Einige Stimmen gehen zudem von einem Rangverhältnis zwischen den Rechtsgütern aus, wobei teilweise ein Vorrang der Individualrechtsgüter, teilweise ein Vorrang der Staatsschutzgüter betont wird. Die Einordnung in den Abschnitt „Gefährdung des demokratischen Rechtsstaates“ sowie der Wille des Gesetzgebers belegen jedoch die vorrangig staatsschutzbezogene Ausrichtung der Vorschrift. (...)“

Diese Defizite sind erheblich, behindern die *strafrechtliche Praxis* jedoch nur peripher, da die Gefährdung des jeweiligen Gutes bei abstrakten Gefährdungsdelikten kein Tatbestandsmerkmal, sondern nur ein außertatbestandliches gesetzgeberisches Motiv bildet. Das SächsPVDG-E erhebt das Schutzgut jedoch zum Merkmal im *Tatbestand* von Standardmaßnahmen, indem es verlangt, dass „im Einzelfall tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut“ bestehen muss. Die Feststellung einer dergestalt „konkretisierten Gefährdung“ wird sich aber mit Blick auf die genannten, überaus vagen Güter vielfach kaum mit Bestimmtheit treffen lassen. Die Unbestimmtheit der strafrechtlichen Schutzgüter schlägt hier demnach auf die Befugnisnormen durch. Dies birgt die Gefahr, dass die Eingriffsvoraussetzungen

³ Hefendehl, ZIS 2012, S. 506 f.; Zöller, ZStW 135 (2023), S. 837.

⁴ Näher Hefendehl, ZIS 2012, S. 506 ff. m.w.N.

einen Grad der Unbestimmtheit aufweisen, der dem allgemeinen rechtsstaatlichen Bestimmtheitsgrundsatz (Art. 20 III GG) zuwiderläuft.

Eine vollends befriedigende Lösung für dieses – vom sächsischen Gesetzgeber nicht zu vertretende – Problem ist nicht in Sicht. Es könnte jedoch durch einen Zusatz zu § 4 Nr. 6 SächsPVDG-E zumindest abgeschwächt werden. Dieser müsste klarstellen, dass zur Rechtfertigung von Standardmaßnahmen, die auf Nr. 6 verweisen, stets erforderlich ist, dass tatsächliche Anhaltspunkte für eine Gefahr solcher geschützten Rechtsgüter vorliegen, die ihrer Natur nach einer konkreten Gefährdung überhaupt zugänglich sind. Damit würde verdeutlicht, dass allzu vage, ausgreifende und unabgrenzbare Schutzziele für die Feststellung einer „konkretisierten Gefährdung“ nicht in Ansatz gebracht werden dürfen, sondern nur „konkret gefährdbare“ Rechtsgüter. Dies hätte zwar zur Folge, dass die betreffenden Standardmaßnahmen zur Verhinderung mancher abstrakter Gefährdungsdelikte mit überaus vagen Schutzzwecken nicht zur Anwendung gebracht werden könnten. Dieser Preis wäre zur Wahrung der Rechtssicherheit und zur Vermeidung von Verfassungsbeschwerden zum SächsVerfGH und BVerfG jedoch zu zahlen.

Formulierungsvorschlag:

„Vorfeldstraftat: Straftatbestand, der Verhaltensweisen erfasst, die in räumlicher oder zeitlicher Hinsicht noch vor einer konkreten oder konkretisierten Gefährdung oder gar Verletzung der geschützten Individualrechtsgüter oder Kollektivrechtsgüter liegen können und vom Gesetzgeber entweder aufgrund ihrer abstrakten Gefährlichkeit oder als Vorbereitungshandlungen unter Strafe gestellt werden.

Soweit dieses Gesetz Maßnahmen zur Verhinderung von Vorfeldstraftaten davon abhängig macht, dass im Einzelfall tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen, gilt: Als Rechtsgut in diesem Sinne kommen nur Individualrechtsgüter oder Kollektivrechtsgüter in Betracht, die ihrer Natur nach einer konkreten Gefährdung zugänglich sind. Unklare und unabgrenzbare Schutzrichtungen genügen nicht.“

Münster, 14. November 2025

Lothar Beste

SÄCHSISCHE DATENSCHUTZ- UND TRANSPARENZBEAUFTRAGTE
Postfach 11 01 32 | 01330 Dresden

Ihr/-e Ansprechpartner/-in
Thomas Mauersberger

SMI Referat Polizeirecht <Polizeirecht@smi.sachsen.de>

Durchwahl
Telefon +49 351 85471-140
Telefax +49 351 85471-109

per E-Mail: Anhoerung.SaechsPVDG@smi.sachsen.de

post@sdtb.sachsen.de*

Aktenzeichen
(bitte bei Antwort angeben)
4-2801/24/1-2025/26373

Dresden,
12. November 2025

Anhörungsverfahren zur Novellierung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG)

Schreiben vom 6.10.2025, Zeichen: 36-2002/25/14

Sehr geehrte Damen und Herren,

für die Übersendung des Entwurfs des Gesetzes zur Änderung polizeirechtlicher Vorschriften und die Gelegenheit zur Stellungnahme danke ich.

Im Schreiben vom 6. Oktober 2025 wird völlig zutreffend darauf hingewiesen, dass die Gewährleistung von Sicherheit und Freiheit eine Kernaufgabe unseres demokratischen Rechtsstaates ist.

Bevor ich zu einzelnen Vorschriften des Gesetzentwurfs Stellung nehme, möchte ich aus datenschutzrechtlicher Sicht anmerken, dass die Gewährleistung von Sicherheit und Freiheit, die beide Belange gleichermaßen berücksichtigt, nicht nur Aufgabe, sondern auch Voraussetzung und Wesensmerkmal eines demokratischen Rechtsstaats sind. Befugnisse des Staats, die Sicherheit gewährleisten sollen, aber zugleich Freiheitsrechte der Menschen beschränken, müssen daher hohen, verfassungsrechtlich verankerten Anforderungen an Bestimmtheit, Geeignetheit und Verhältnismäßigkeit entsprechen.

Der Gesetzentwurf enthält begrüßenswerte Änderungen, insbesondere in Umsetzung verfassungsgerichtlicher Rechtsprechung. Dies betrifft etwa die Präzisierung des Begriffs der Vorfeldstraftat und die Bestimmung der Voraussetzungen für eine vorsorgliche Speicherung personenbezogener Daten für künftige Verfahren oder die Schaffung von Rechtsgrundlagen für Maßnahmen, die bislang rechtstaatlich bedenklich auf die polizeiliche Generalklausel zur Verarbeitung personenbezogener Daten gestützt wurden, zum Beispiel für die Speicherung von personenbezogenen oder ermittlungsunterstützenden Hinweisen zu einer bestimmten Person. Ausdrücklich zu begrüßen ist auch die Streichung der Befugnis zur Ausschreibung von Kontakt- und Begleitpersonen aus Gründen der Verhältnismäßigkeit.

Hausanschrift:
Sächsische
Datenschutz- und
Transparenzbeauftragte
Maternistraße 17
01067 Dresden

www.datenschutz.sachsen.de

Verkehrsanbindung:
Zu erreichen mit den S-Bahn-Linien S1 und S2 sowie den Straßenbahnlinien 7, 10 und 12 (Haltestelle S-Bf. Freiburger Straße)

*Informationen über die Verarbeitung Ihrer personenbezogenen Daten und zum Zugang für verschlüsselte E-Mails finden Sie im Internet unter www.datenschutz.sachsen.de/datenschutzerklaerung.html.

Andererseits finden sich im Gesetzentwurf Bestimmungen zu Befugnissen, die eine enorme Eingriffstiefe aufweisen, ohne zugleich wirksame eingriffsmindernde Vorkehrungen zu treffen – beispielhaft seien die automatisierte Datenanalyse, die Nutzung personenbezogener Daten für das Trainieren und Testen selbstlernender KI-Systeme oder die Videoüberwachung des fließenden Verkehrs mit Bildaufzeichnung des Fahrzeugführers zur Verhütung einer Ordnungswidrigkeit genannt –, die ohne Begründung der Erforderlichkeit die Speicherfrist für Aufzeichnungen der Videoüberwachung des öffentlichen Raums und damit den Umfang der verarbeiteten Daten verdoppeln, oder die es erlauben, polizeilich gespeicherte personenbezogene Daten privaten Unternehmen zur Weiterentwicklung und Vermarktung ihrer Produkte zugänglich zu machen (selbstlernende KI-Systeme).

In diesen Fällen muss ebenso wie bei Befugnissen, die die Einbeziehung von umfangreichen polizeifremden und nahezu unbegrenzten, auch privaten Datenbeständen vorsehen (automatisierte Datenanalyse und Abgleiche mit dem Internet), besonders kritisch hinterfragt werden, ob entsprechende Maßnahmen geeignet und erforderlich wären, den angestrebten Zweck zu erreichen, und in ihrer Beeinträchtigung der Grundrechte der betroffenen Personen die gebotene Verhältnismäßigkeit wahren.

Aus datenschutzrechtlicher Sicht bestehen bezüglich einiger (neuer) Befugnisse erhebliche Zweifel daran, dass Sicherheit – im Sinne eines handlungsfähigen, Gefahren abwehrenden Staates – und Freiheit – im Sinne einer Ausübung von Grundrechten frei von staatlicher Einwirkung – in einem verfassungsrechtlich gebotenen ausgewogenen Verhältnis stehen.

Zu einzelnen Vorschriften (Angaben von Vorschriften ohne Bezeichnung des Gesetzes beziehen sich auf den vorgelegten Entwurf des überarbeiteten SächsPVDG):

I. Einsatz von Bodycams in Wohnungen - § 57 Abs. 4, 5, 6, 7, 8

Die Vorschriften weisen, insbesondere in der Variante des Einsatzes von Bodycams in Wohnungen zum Schutz der eigenen Person, also der eingesetzten Beamten, eine große Nähe zu bzw. Überschneidungen mit der Regelung in § 65 Abs. 3 SächsPVDG auf (Einsatz technischer Mittel zur Datenerhebung in oder aus Wohnungen ausschließlich zum Schutz der bei einem polizeilichen Einsatz in Wohnungen tätigen Personen). Dies sollte vor allem hinsichtlich einer strengen Zweckbindung für die Verwendung von Aufzeichnungen zu einer Harmonisierung der Normen führen, die mit der Entwurfsregelung noch nicht erreicht wird.

Mit der Schaffung einer Rechtsgrundlage für den Einsatz von sog. Bodycams in Wohnungen in **§ 57 Abs. 4 Satz 2** und die Aufzeichnung entsprechender Bilder in **§ 57 Abs. 5** soll die Nutzung der Technik auf den verfassungsrechtlich besonders geschützten Bereich der Wohnung erweitert werden.

Die verfassungsrechtlichen Vorgaben für Eingriffe in die Unverletzlichkeit der Wohnung nach Art. 13 Abs. 7 GG und Art. 30 Abs. 3 SächsVerf setzt der Entwurf um, indem er als Eingriffsschwelle das Vorliegen einer dringenden Gefahr für Leib oder Leben der eingesetzten Polizeibeamten oder Dritter bestimmt, wobei nach Abs. 4 Satz 2 das sog. Pre-Recording bereits zulässig sein soll, wenn „dies mit hinreichender Wahrscheinlichkeit zur Abwehr einer dringenden Gefahr für Leib oder Leben der eigenen oder einer dritten Person erforderlich ist“.

Eine solche „Aufweichung“ der Voraussetzung des Vorliegens einer dringenden Gefahr sehen Art. 13 Abs. 7 GG und Art. 30 Abs. 3 SächsVerf nicht vor.

Da bereits das Pre-Recording in Wohnungen ein Eingriff in deren Unverletzlichkeit ist und die Aufnahmen aus dem Zwischenspeicher längerfristig gespeichert werden, wenn die Gefahrenlage anhält (Abs. 5), muss schon das Pre-Recording zur Verhütung einer dringenden Gefahr erforderlich sein, um die verfassungsrechtlichen Anforderungen zu erfüllen. Eine nur hinreichende Wahrscheinlichkeit der Erforderlichkeit zur Abwehr einer dringenden Gefahr ist nicht ausreichend.

Bereits das Pre-Recording in Wohnungen nach § 57 Abs. 4 Satz 2 ist verfassungsrechtlich nur zur Abwehr einer dringenden Gefahr einer – mindestens – dringenden Gefahr zulässig. Die Vorschrift sollte entsprechend geändert werden.

Unklar ist, welche Konsequenz mit der in der Begründung zu § 57 Abs. 4 getroffenen Feststellung verbunden sein soll, dass die Dringlichkeit der Gefahr im Sinne des Artikel 13 Absatz 7 GG sich nicht auf die Wahrscheinlichkeit des Schadenseintritts beziehe, sondern auf den Umfang des drohenden Schadens.

Wird im SächsPVDG ein Begriff verwendet, der im SächsPVDG selbst definiert wird – für die dringende Gefahr ist dies in § 4 Nr. 3 Buchst. d SächsPVDG der Fall – gilt diese Legaldefinition. Danach ist eine dringende Gefahr eine im Hinblick auf das Ausmaß des zu erwartenden Schadens und die Wahrscheinlichkeit des Schadenseintritts erhöhte Gefahr. Insofern ist beim Einsatz von Bodycams in Wohnungen die Wahrscheinlichkeit des Schadenseintritts sehr wohl zu berücksichtigen.

Nicht nachvollziehbar ist die in **Abs. 5 Satz 3** vorgenommene Anordnung der automatisierten Löschung nach 60 Sekunden für Aufzeichnungen nach Abs. 5 Satz 1 und 2.

Abs. 5 Satz 1 und 2 erlauben gerade die Aufzeichnung und Speicherung über 60 Sekunden (Zwischenspeicher im Pre-Recording). Abs. 5 Satz 3 erscheint insofern deplatziert und wäre im Hinblick auf den Regelungsinhalt – insbesondere die automatisierte Löschung und den Vorbehalt einer in Abs. 5 geregelten Aufzeichnung – als Satz 4 in Abs. 4 passender verortet.

Abs. 6 Satz 2 ff. sollen den **Schutz des Kernbereichs privater Lebensgestaltung** sicherstellen. Nicht nachvollziehbar ist, weshalb sich die Regelungen ausdrücklich (nur) auf den Einsatz von Bodycams in Wohnungen beziehen. Der Kernbereich privater Lebensgestaltung genießt einen absoluten Schutz vor staatlichen Eingriffen, wobei es unerheblich ist, wann und wo er tangiert wird. Es gibt keine zeitlichen oder örtlichen Vorgaben oder Beschränkungen. Denkbar sind daher auch Eingriffe in den Kernbereich privater Lebensgestaltung außerhalb von Wohnungen.

Vor diesem Hintergrund sollte in Abs. 6 Satz 2 und 4 die ausdrückliche Anknüpfung an Abs. 5 Satz 2 gestrichen werden; der Verweis auf Maßnahmen nach Abs. 5 wäre ausreichend, aber auch verfassungsrechtlich geboten.

Nach **Abs. 7 Satz 2** soll die Mitteilung über das Starten der Aufzeichnung bei Gefahr im Verzug unterbleiben können. Sofern der Einsatz von Bodycams deeskalierend und warnend wirken soll, ist der Verzicht auf eine Mitteilung möglicherweise kontraproduktiv, da gerade die Mitteilung über eine Aufzeichnung des Geschehens den betroffenen Personen die Möglichkeit gibt, einen bevorstehenden Grundrechtseingriff zu erkennen und ihr Verhalten anzupassen. Polizeiliche Maßnahmen können in konkreten Gefahrenlagen

präventive Wirkung nur entfalten, wenn sie transparent erfolgen und den potentiell Betroffenen bekannt sind. Andernfalls werden sie zu bloßen Maßnahmen der Beweissicherung, die eher repressiven Charakter aufweisen.

Abs. 8 Satz 5 stellt die weitere Verarbeitung von Daten aus Maßnahmen nach Abs. 5 Satz 2 unter den Vorbehalt der richterlichen Feststellung der Rechtmäßigkeit der Maßnahme. Die Vorschrift orientiert sich offenkundig an Art. 13 Abs. 5 Satz 2 GG, der einen solchen Richtervorbehalt für die Verwendung von Erkenntnissen vorsieht, die beim Einsatz technischer Mittel ausschließlich zum Schutze der bei einem Einsatz in Wohnungen tätigen Personen erlangt wurden.

Allerdings beschränkt Abs. 8 Satz 5 die Weiterverarbeitung der mittels Bodycam in Wohnungen aufgenommenen Daten in keiner Weise. Mit Blick auf den hohen verfassungsrechtlichen Schutz der Unverletzlichkeit der Wohnung ist eine fehlende Begrenzung der Verwendung der Aufzeichnungen innerhalb der vorgesehenen Speicherdauer von einem Monat (Abs. 8 Satz 2) äußerst bedenklich. Denkbar wäre danach eine Nutzung der Aufnahmen aus Wohnungen auch für die automatisierte Datenanalyse, Aus- und Fortbildungszwecke, für Forschungszwecke, für archivarische Zwecke sowie zum Trainieren und Testen von KI-Systemen.

Wie eingangs erwähnt, weisen die Vorschriften in § 57 Abs. 4 und 5 und in § 65 Abs. 3 SächsPVDG Übereinstimmungen insbesondere hinsichtlich der Eröffnung des Schutzbereichs von Art. 13 GG auf. Während aber für eine weitere Verwendung der Aufzeichnungen in beiden Konstellationen – und in Übereinstimmung mit Art. 13 Abs. 5 Satz 2 GG – die richterliche Feststellung der Rechtmäßigkeit der Maßnahme Voraussetzung ist, fehlt die in § 65 Abs. 3 Satz 2 SächsPVDG bestimmte enge Zweckbindung in § 57 Abs. 8 Satz 5 gänzlich.

Abs. 8 Satz 5 sollte daher an § 65 Abs. 3 Satz 2 SächsPVDG angepasst werden, um eine einheitliche und verfassungskonforme Rechtsanwendung sicherzustellen. Eine zweckändernde Verwendung der Aufzeichnungen sollte dementsprechend nur unter den Voraussetzungen des § 79 Absatz 2 und 3 Satz 1 SächsPVDG (künftig § 79a Absatz 2 und 3 Satz 1) zulässig sein.

II. Videoüberwachung des öffentlichen Verkehrsraums zur Verhütung einer Ordnungswidrigkeit - § 57 Abs. 9

Die Vorschrift soll der Polizei erlauben, offen Bildaufnahmen von Fahrzeugkennzeichen und Fahrzeugführern an bestimmten Streckenabschnitten oder Verkehrsknoten zu erheben und aufzuzeichnen, um Verstöße von Verkehrsteilnehmern gegen § 23 Abs. 1a StVO (Handynutzung am Steuer) zu verhüten. Voraussetzung sollen tatsächliche Anhaltspunkte dafür sein, dass an den betreffenden Orten regelmäßig gegen die Vorschrift verstoßen wird oder es sich in sonstiger Weise um einen Bereich mit besonderer Unfallträchtigkeit handelt.

Die Entwurfsregelung begegnet schwersten datenschutz- und verfassungsrechtlichen Bedenken. Die Diskrepanz zwischen der Intensität der Grundrechtseingriffe – sowohl hinsichtlich der Streubreite, also der Zahl der betroffenen Personen, als auch hinsichtlich der verarbeiteten Daten (u.a. Bilder der Fahrzeugführer) – und dem Normzweck, der Verhütung eines abstrakten Gefährdungsdelikts unterhalb der Schwelle einer Straftat, ist eklatant.

In der Begründung wird die Vorschrift als eine Regelung beschrieben, „die der Polizei die präventive Überwachung von fahrzeugführenden Personen ermöglicht, die infolge des Begehens einer bedeutenden Ordnungswidrigkeit erhebliche Gefährdungen für den Straßenverkehr und damit für Leib und Leben hervorrufen“. Diese Aussage ist grundfalsch und ebenso irreführend wie die der Hinweis auf die „verdachtslose Überwachung des betreffenden Verkehrsverstößes“. Tatsächlich handelt es sich gerade nicht um die „Überwachung von Verstößen“ oder die Überwachung von Fahrzeugführern, die eine „bedeutende Ordnungswidrigkeit begehen“, sondern um die verdachtslose Überwachung sämtlicher Fahrzeugführer in dem von den Kameras erfassten Bereich, wobei ganz sicher davon auszugehen ist, dass sich nahezu alle Betroffenen rechtstreu verhalten. Die Maßnahme unterscheidet sich damit wesentlich von der repressiven Erfassung von Geschwindigkeits- und Rotlichtverstößen, die durch technische Voreinstellungen ausnahmslos an einen Anfangsverdacht anknüpfen, wodurch tatsächlich nur „Verdächtige“ betroffen werden und ordnungsgemäß agierende Verkehrsteilnehmer unbeobachtet bleiben. Das mag im Hinblick auf den prinzipiellen Unterschied zwischen präventiven und repressiven Maßnahmen eine Selbstverständlichkeit sein, zeigt aber auch, dass die Aufdeckung von Verkehrsordnungswidrigkeiten und der damit einhergehende Erziehungseffekt auf grundrechtsschonende Weise erzielt werden können.

Der Verstoß gegen das Verbot der Handynutzung am Steuer nach § 23 Abs. 1a StVO ist ein abstraktes Gefährdungsdelikt und auch dann vollendet, wenn ein konkretes Rechtsgut zu keinem Zeitpunkt gefährdet wurde. Damit bewegt sich die Vorschrift in einem Regelungsbereich, den der Sächsische Verfassungsgerichtshof in seiner Prüfung von Vorschriften des Sächsischen Polizeivollzugsdienstgesetzes intensiv beleuchtet hat ((Verfassungsgerichtshof des Freistaates Sachsen, Urteil vom 25. Januar 2024 – Vf. 91-II-19).

Das Gericht hat u.a. folgende Feststellung getroffen: „Entscheidet sich der Gesetzgeber im Bereich der Gefahrenabwehr dafür, auf bestimmte Straftaten zu verweisen, deren Verhinderung die Maßnahme dienen soll, muss sichergestellt sein, dass nicht auf Straftaten verwiesen wird, die Situationen erfassen, in denen die Strafbarkeitsschwelle durch die Pönalisierung von Vorbereitungshandlungen oder bloßen Rechtsgutsgefährdungen ins Vorfeld von Gefahren verlagert wird (vgl. BVerfG, Urteil vom 2. März 2010, BVerfGE 125, 260 [329]; vgl. zur Frage der Übermittlung erhobener Daten BVerfG, Urteil vom 19. Mai 2020, BVerfGE 154, 152 [269 Rn. 221]; vgl. Beschluss vom 9. Dezember 2022 – 1 BvR 1345/21 – juris Rn. 95). Diese Delikte sind verwirklicht, ohne dass das strafbewehrte Handeln eine konkrete Gefahr für das geschützte Rechtsgut auslöst“ (SächsVerfGH a.a.O., Rn. 162, juris).

In Umsetzung der Entscheidung des Sächsischen Verfassungsgerichtshofs soll der Begriff der Vorfeldstraftat legal definiert werden (§ 4 Nr. 6); Eingriffsschwellen für Erhebungsbefugnisse knüpfen an tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut an (z.B. § 61 Abs. 1 Satz 2, § 62a Abs. 1 Satz 2, § 62b Abs. 1 Satz 4 usw.).

In krassem Widerspruch dazu steht die Regelung des § 57 Abs. 9, die der Verhütung von Ordnungswidrigkeiten (!) dienen soll, die abstrakte Gefährdungsdelikte sind; auf eine konkrete Gefahr für bestimmte Rechtsgüter soll es gerade nicht ankommen.

Die verdachtslose Überwachung des öffentlichen Straßenverkehrs ist ein Grundrechtseingriff von erheblichem Gewicht. Das Bundesverfassungsgericht hat wiederholt polizeirechtliche Regelungen zur automatisierten Kennzeichenerfassung und -kontrolle überprüft und dabei u.a. festgestellt, dass

- das Eingriffsgewicht erhöhend sich solche Kontrollen dadurch auszeichnen, dass sie sich schon ihrem Prinzip nach nicht auf Personen beschränken, die objektiv in einer Gefahrenlage verfangen sind, sondern sich auf eine unbestimmte Vielzahl von Personen erstrecken, die von vornherein hierzu keinerlei Anlass gegeben haben (BVerfG, Beschluss vom 18. Dezember 2018 – 1 BvR 142/15 –, BVerfGE 150, 244-309, Rn. 98), und
- es dem erheblichen Eingriffsgewicht automatisierter Kraftfahrzeugkennzeichenkontrollen entspricht, dass sie zu ihrer Rechtfertigung jeweils auf Gründe gestützt werden müssen, die dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht oder sonst einem vergleichbar gewichtigen öffentlichen Interesse dienen (BVerfG a.a.O., Rn. 99).

— Eine Minderung des Eingriffsgewichts der automatisierten Kraftfahrzeugkennzeichenkontrolle sieht das Bundesverfassungsgericht u.a. darin, dass

- sich die Kontrolle allein auf Kennzeichen, nicht aber unmittelbar auf persönliche Merkmale oder Eigenschaften einer Person bezieht (BVerfG a.a.O., Rn. 97),
- nur Ort, Datum, Uhrzeit und Fahrtrichtung erfasst werden, nicht aber die Personen oder die Kraftfahrzeuge (BVerfG a.a.O., Rn. 97), und
- der Datenabgleich in Sekundenschnelle durchgeführt wird und die erfassten Daten im Nichttrefferfall sofort vollständig wieder gelöscht werden, ohne einer Person bekannt zu werden (BVerfG a.a.O., Rn. 97).

— § 57 Abs. 9 soll lediglich der Verhütung einer leichten bis allenfalls mittleren Ordnungswidrigkeit dienen, ohne dass es auf eine konkrete Gefährdung eines Rechtsguts ankäme. Das durch die Betroffenheit einer großen Zahl von Personen, die keinen Anlass für eine polizeiliche Erfassung gegeben haben, begründete erhebliche Eingriffsgewicht wird nicht etwa durch die Beschränkung der erfassten Informationen gemindert, sondern im Vergleich zur automatisierten Kennzeichenkontrolle noch einmal erhöht, indem Bilder von Fahrzeug, Kennzeichen und Fahrzeugführer erhoben und aufgezeichnet werden sollen. Darüber hinaus sieht § 57 Abs. 9 im Gegensatz zur automatisierten Kennzeichenkontrolle keine gesetzliche Anordnung der sofortigen, technisch spurlosen und automatisierten Löschung im Nicht-Trefferfall vor (vgl. § 58 Abs. 3 Satz 4), sondern nur eine unverzügliche Löschung, die spätestens bei Beendigung der Maßnahme vorzunehmen ist, wobei eine Bestimmung zur Dauer der Maßnahme gänzlich fehlt.

— Die Vorschrift entspricht offensichtlich weder den Vorgaben des Sächsischen Verfassungsgerichtshofs noch den durch das Bundesverfassungsgericht benannten verfassungsrechtlichen Anforderungen; die Eingriffsbefugnis ist klar unverhältnismäßig.

Überdies erweist sich die Zweckbindung in **§ 57 Abs. 9 Satz 4** als **wirkungslos**, sofern die Bildaufzeichnungen in strafprozessualen Ermittlungsverfahren benötigt und angefordert werden. Eine landesrechtliche Verwendungsbeschränkung auf die Verfolgung und Ahndung von Verstößen gegen § 23 Abs. 1a StVO entfaltet keine Wirkung gegenüber bundesrechtlichen Ermittlungsbefugnissen (§ 161 Abs. 1 StPO), da es an einer entsprechenden bundesgesetzlichen Verwendungsregelung bzw. -beschränkung fehlt (vgl. § 160 Abs. 4 StPO). Als eingriffsmindernd kann Satz 4 daher nicht angesehen werden.

Angesichts der auf der Hand liegenden Unverhältnismäßigkeit der Befugnis sei nur am Rande erwähnt, dass die vorgesehene Offenheit, also Erkennbarkeit der Videoüberwachung des fließenden Straßenverkehrs dann kaum umzusetzen wäre, wenn sie mittels

Drohnen erfolgen soll; § 71 Abs. 1 Satz 1 Nr. 2 sieht diese Möglichkeit ausdrücklich für Maßnahmen nach § 57 Abs. 1 bis 3 und Abs. 9 vor.

§ 57 Abs. 9 ist offensichtlich verfassungswidrig und sollte ersatzlos gestrichen werden.

III. Zweimonatige Aufbewahrungsfrist für Bildaufzeichnungen – § 57 Abs. 12

Nach § 57 Abs. 12 sollen Bildaufzeichnungen, die nach **§ 57 Abs. 2 oder 3** gefertigt wurden, künftig bis zu zwei Monate aufbewahrt werden können, auch wenn keine Notwendigkeit ihrer Verwendung für die polizeiliche Aufgabenerfüllung erkennbar ist (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, können Aufzeichnungen selbstverständlich – wie bisher – weiterverwendet werden und unterliegen dann den jeweils einschlägigen Aufbewahrungsfristen).

Im Gegensatz zur unzutreffenden Begründung, wonach Abs. 12 „der Regelung des bisherigen Absatz 10 (entspricht)“, geht mit der Vorschrift eine **Verdoppelung der bisherigen Aufbewahrungsfrist** einher. Der bislang geltende § 57 Abs. 10 SächsPVDG sieht eine Aufbewahrungsfrist von einem Monat vor.

Ein polizeifachlicher Bedarf für die Ausweitung der Frist ist weder dargelegt noch erkennbar. In der Praxis schöpft die Polizei bereits die Monatsfrist nach § 57 Abs. 10 SächsPVDG bei weitem nicht aus.

Dem steht mit der beabsichtigten Verdopplung dieser Frist eine massive Vertiefung des Eingriffs in die Rechte der von Videoüberwachungen nach § 57 Abs. 2 oder 3 betroffenen Personen gegenüber. Während Aufzeichnungen bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen unter freiem Himmel nach § 57 Abs. 2 an ein bestimmtes Verhalten anknüpfen und Personen betreffen, „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“, und insofern hinsichtlich der Zahl erfasster Personen überschaubar sein dürften, knüpfen Aufzeichnungen nach § 57 Abs. 3 lediglich an Örtlichkeiten an und erfassen zum weitaus größten Teil bzw. nahezu ausschließlich Personen, die keinerlei Anlass für eine polizeiliche Befassung mit ihnen geben (Passanten, Berufspendler, Touristen, Anwohner an Örtlichkeiten nach Abs. 3 Nr. 1 oder auf Plätzen, auf Straßen oder in Parks, die als Kriminalitätsschwerpunkte nach Abs. 3 Nr. 2 überwacht werden).

Eine verfassungsrechtlich tragfähige Rechtfertigung für die massive Ausweitung der Aufbewahrungsfrist, die den in hochauflösenden Bildaufzeichnungen liegenden erheblichen Eingriff in die Rechte dieser sich rechtstreu verhaltenden Personen noch einmal vertieft, ist nicht ersichtlich.

Eine zusätzliche Intensivierung des Grundrechtseingriffs liegt in den Verwendungsmöglichkeiten, die der Gesetzentwurf für Bildaufzeichnungen nach § 57 Abs. 2 und 3 eröffnet,

die künftig ohne Anlass für eine weitere Verwendung zwei Monate aufbewahrt werden dürfen.

Hierzu gehören etwa die Auswertung der Bilder hinsichtlich verdächtiger Bewegungs- oder Gegenstandsmuster nach § 57a Abs. 1 Satz 1 und nach § 57a Abs. 1 Satz 3 die Kennzeichnung und automatisierte Nachverfolgung in vorliegenden Bildaufzeichnungen (die an verschiedenen Stellen im Gesetzentwurf vorgesehene biometrische Echtzeit-Fernidentifizierung betrifft definitionsgemäß Vorgänge, in denen die Erfassung biometrischer Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen, Art. 3 Nr. 42 der Verordnung (EU) 2024/1689 – KI-VO), der nachträgliche biometrische Abgleich mit öffentlich zugänglichen Daten aus dem Internet nach § 62b oder die Nutzung für Training und Tests von lernenden IT-Systemen (KI) nach § 79c.

Rechtsreue Bürger sind damit potentiell zwei Monate lang – im Fall der Nutzung der Daten für das KI-Training nach § 79c sogar auf unbegrenzte Dauer – einer ganzen Reihe von teils massiven Grundrechtseingriffen ausgesetzt, die sich an ihren rechtmäßigen Aufenthalt an bestimmten Orten anschließen und obwohl sie keinerlei Anlass für eine polizeiliche Befassung mit ihnen gesetzt haben.

Eine zweimonatige Speicherfrist für Aufzeichnungen nach § 57 Abs. 2 und 3 ist unverhältnismäßig. Angesichts der erweiterten Verwendungsmöglichkeiten sollte die derzeit nach § 57 Abs. 10 SächsPVDG geltende Aufbewahrungsfrist von einem Monat nicht verdoppelt, sondern, im Gegenteil, erheblich verkürzt werden.

IV. „Intelligente Videoüberwachung“ - § 57a

Abs. 1 Satz 1 Mustererkennung

Die Vorschrift soll für Aufnahmen nach § 57 Abs. 2 und 3 den Einsatz von Bildanalyse-Software auf der Grundlage künstlicher Intelligenz (KI) ermöglichen, um Bewegungsmuster bei bzw. von Personen zu erkennen, die auf die Begehung einer Straftat hindeuten, bzw. Waffen oder gefährliche Gegenstände zu identifizieren.

Die automatisierte Analyse der personenbezogenen Aufnahmen nach § 57 Abs. 2 und 3 vertieft den bereits durch die Aufnahme selbst vollzogenen Eingriff in die Rechte der betroffenen Personen, auch wenn der Begründung insofern zuzustimmen ist, als der zusätzliche Eingriff noch nicht zur Identifizierung der betroffenen Personen führt und – für sich genommen – eher geringfügig ist.

Von Bedeutung ist in diesem Zusammenhang, dass die technikoffen formulierte Vorschrift laut Begründung nur den Einsatz bereits austrainierter und ausgelerner Systeme erlauben soll. Die Modelle sind, so die Begründung, unveränderlich vorprogrammiert und lernen nicht auf Grundlage der polizeilichen Daten (hier der Bildaufnahmen) weiter.

Diese Präzisierung ist zu begrüßen, unterstreicht sie doch den Charakter der Technik als rein unterstützendes Werkzeug innerhalb der Wahrnehmung einer konkreten polizeilichen Aufgabe.

Freilich wird dieser positive Ansatz des Gesetzentwurfs wieder vollständig entwertet und zunichtegemacht, wenn § 79c die Verarbeitung nahezu sämtlicher personenbezogener Daten, die der Polizei vorliegen, zum Trainieren und Testen von lernenden Systemen

bzw. KI-Modellen, ggf. sogar durch Dritte, erlaubt und unter Umständen Dritten die Nutzung der mit personenbezogenen Daten der sächsischen Polizei trainierten Modelle für eigene Zwecke einräumt. Aufgrund der völlig offenen Formulierung in § 79c Abs. 1 sind davon auch Aufnahmen nach § 57 Abs. 2 und 3 umfasst.

Vor diesem Hintergrund sollte der in der Begründung zum Ausdruck kommende Regelungswille Niederschlag finden, indem die Anwendung lernender KI-Systeme in der Vorschrift selbst ausdrücklich untersagt wird (dazu mehr unter XVIII. zu § 79c).

Abs. 1 Satz 1 enthält, im Gegensatz zu Satz 4, der nur eine biometrische Echtzeit-Fernidentifizierung erlauben soll (aber keine retrograde biometrische Fernidentifizierung), keine zeitliche Komponente. Das heißt, dass grundsätzlich nach § 57 Abs. 2 und 3 aufgezeichnete Bilder auch rückwirkend hinsichtlich Bewegungs- und Gegenstandsmustern analysiert werden können, künftig also bis zu zwei Monate lang (§ 57 Abs. 12). Angesichts des Umstandes, dass der von Maßnahmen nach Satz 1 betroffene Datenbestand nahezu ausschließlich Daten von Personen umfasst, die keinen Anlass für eine polizeiliche Befassung mit ihnen geben (s.o.), sollte die Musteranalyse aus Gründen der Verhältnismäßigkeit – aber auch zur Harmonisierung mit der in Echtzeit vorzunehmenden Anwendung in Satz 4 – auf eine Live-Analyse bzw. eine Analyse von Bildern ohne erhebliche Verzögerung nach ihrer Entstehung beschränkt werden.

Abs. 1 Satz 4 – biometrische Echtzeit-Fernidentifizierung bei gegenwärtiger Gefahr

Für den Fall, dass im Anschluss an die automatisierte Erkennung eines auf eine Gefahr hindeutenden Musters (Satz 1) in absehbarer Zeit mit hinreichender Wahrscheinlichkeit mit der Begehung einer Straftat von erheblicher Bedeutung gerechnet werden kann (Satz 2), weshalb eine Kennzeichnung und automatisierte Nachverfolgung der verantwortlichen Person in den der Polizei vorliegenden Bildübertragungen und -aufzeichnungen vorgenommen werden darf (Satz 3), soll nach Satz 4 „eine biometrische Echtzeit-Fernidentifizierung von in öffentlich zugänglichen Bereichen erhobenen personenbezogenen Daten anhand des Datenbestandes der polizeilichen Auskunft- und Fahndungssysteme“ durchgeführt werden können, „wenn eine erhebliche gegenwärtige Gefahr für Leib oder Leben einer Person vorliegt, sofern die Abwehr dieser Gefahr auf diese Weise unbedingt erforderlich ist“.

Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen ist als Maßnahme von enormer Eingriffstiefe gemäß Art. 5 Abs. 1 Buchst. h KI-VO grundsätzlich verboten; Ausnahmen sind nur unter hohen Voraussetzungen vorgesehen. Satz 4 bezieht sich auf eine solche Ausnahme: Art. 5 Abs. 1 Buchst. h Doppelbuchst. ii KI-VO. Auch wenn die Gefahrbegriffe in Art. 5 Abs. 1 Buchst. h Doppelbuchst. ii KI-VO einerseits und in Satz 4 andererseits sich geringfügig unterscheiden, ist der hier verwendete Begriff der „erheblichen gegenwärtigen Gefahr“ vom Gefahrbegriff der KI-VO umfasst.

Eine gegenwärtige Gefahr ist nach der Legaldefinition in § 4 Nr. 3 Buchst. b SächsPVDG eine Sachlage, bei der das schädigende Ereignis bereits begonnen hat oder unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht.

Angesichts der Anwendungsvoraussetzungen bestehen erhebliche Zweifel an der Geeignetheit der Norm und damit an ihrer Verhältnismäßigkeit.

Der Grundsatz der Verhältnismäßigkeit verlangt, dass ein Grundrechtseingriff von hinreichenden Gründen des Gemeinwohls gerechtfertigt wird, das gewählte Mittel zur Erreichung des Zwecks geeignet und erforderlich ist und bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht der ihn rechtfertigenden Gründe die Grenze des Zumutbaren noch gewahrt ist (Verfassungsgerichtshof des Freistaates Sachsen, Urteil vom 25. Januar 2024 – Vf. 91-II-19 –, Rn. 155, juris).

Es ist nicht ersichtlich, dass die Identifizierung einer Person, von der eine gegenwärtige Gefahr für Leib oder Leben einer Person ausgeht, diese Gefahr abwenden könnte.

Wenn das schädigende Ereignis bereits begonnen hat oder unmittelbar oder in aller nächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht – im vorliegenden Zusammenhang handelt es sich dann um eine akute Lebensgefahr oder schon eingetretene oder unmittelbar bevorstehende körperliche Verletzungen – ist ein sofortiges tatsächliches Einschreiten geboten und alternativlos. Die Polizei verfügt über robuste Befugnisse zur Beendigung der bereits begonnenen oder unmittelbar bevorstehenden Rechtsgutsverletzung. Die Kenntnis der Identität der verantwortlichen Person jedoch ist für die Abwendung des Schadens völlig irrelevant. Die Fernidentifizierung verzögerte mit hoher Wahrscheinlichkeit sogar das gebotene tatsächliche physische Einschreiten, da sie formal anzuordnen ist (Abs. 3).

Irritierend ist vor diesem Hintergrund der letzte Halbsatz von Satz 4, wonach „die Abwehr dieser Gefahr auf diese Weise unbedingt erforderlich“ sein muss. Eine Fernidentifizierung und damit die auch nur eventuelle Kenntniserlangung der Identität der verantwortlichen Person kann offensichtlich keinen Beitrag zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben Dritter leisten. Eine Abwehr der Gefahr „auf diese Weise“, also durch die Fernidentifizierung, ist schlechterdings unmöglich.

Unverständlich bleibt die Begründung, soweit in ihr erläutert wird, dass „dadurch [...] effektiv Menschenleben geschützt und schwere Straftaten verhindert werden [können].“ Die biometrische Fernidentifizierung ist ungeeignet, in einer gegenwärtigen Gefahr Menschenleben zu schützen; im Übrigen soll die Befugnis auch nicht der Verhütung oder Verhinderung einer schweren Straftat dienen.

Die Befugnis nach Abs. 1 Satz 4 ist ungeeignet und damit unverhältnismäßig. Die Regelung sollte ersatzlos gestrichen werden. Gegenwärtige Gefahren müssen physisch vor Ort abgewendet werden.

Abs. 2, 3, 4 – biometrische Echtzeit-Fernidentifizierung und Verfahren

Während Abs. 1 Satz 4 die Anwendung der biometrischen Echtzeit-Fernidentifizierung in einer gegenwärtigen Gefahrenlage vorsieht, senkt **Abs. 2** die Eingriffsschwelle demgegenüber deutlich ab. Zulässig soll die Maßnahme – im Einklang mit Art. 5 Abs. 1 Buchst. h Doppelbuchst. i und ii KI-VO – zur Abwehr einer Gefahr durch einen Terroranschlag oder zur Suche von Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung oder vermissten Personen sein.

Auch wenn die KI-VO den Einsatz von Systemen zur biometrischen Echtzeit-Fernidentifizierung in den in Abs. 2 genannten Fällen für zulässig erklärt, müssen die dazu zu treffenden nationalen Regelungen (vgl. Art. 5 Abs. 5 KI-VO) nationalen Maßstäben des Verfassungsrechts genügen. Im Rahmen der nationalen Gesetzgebung sind zudem zwingend die Bedingungen von Art. 5 Abs. 2 und 3 KI-VO zu berücksichtigen (Art. 5 Abs. 5 Satz 1 KI-VO).

Danach müssen bei der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen folgende Aspekte berücksichtigt werden:

- die Art der Situation, die der möglichen Verwendung zugrunde liegt, insbesondere die Schwere, die Wahrscheinlichkeit und das Ausmaß des Schadens, der entstehen würde, wenn das System nicht eingesetzt würde; und
- die Folgen der Verwendung des Systems für die Rechte und Freiheiten aller betroffenen Personen, insbesondere die Schwere, die Wahrscheinlichkeit und das Ausmaß solcher Folgen.

Abs. 2 bestimmt, dass die Anwendung „unbedingt erforderlich“ sein muss. Wesentliche Erwägungen zu Erforderlichkeit und Verhältnismäßigkeit der Maßnahme sind – lediglich – im Antrag zur richterlichen Anordnung anzugeben (Abs. 3).

Angesichts der Intensität des Grundrechtseingriffs einer biometrischen Echtzeit-Fernidentifizierung ist zu bezweifeln, dass diese gesetzlichen Vorgaben ausreichend sind. Bei gravierenden Grundrechtseingriffen obliegt es mit Blick auf die Wesentlichkeitstheorie dem Gesetzgeber, alle wesentlichen Entscheidungen über grundrechtserhebliche Maßnahmen selbst treffen.

Insbesondere in der Variante der Suche nach Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung oder nach vermissten Personen (Satz 1 Nr. 2) liegen insofern Unklarheiten auf der Hand. Die Website der Polizei Sachsen listet vermisste Personen auf, nach denen seit zehn, zwanzig und in einem Fall seit knapp dreißig Jahren gefahndet wird (<https://www.polizei.sachsen.de/de/3582.htm>).

Der Gesetzgeber ist gefordert, bereits bei der Schaffung der Befugnis ausdrückliche Vorgaben zur Wahrung der Verhältnismäßigkeit in die gesetzliche Vorschrift aufzunehmen. Ein Verweis auf die „unbedingte Erforderlichkeit“ ist dabei unzureichend.

Abs. 2 bezieht sich ausdrücklich auf eine biometrischen Echtzeit-Fernidentifizierung (Art. 4 Nr. 42 KI-VO), lässt also eine nachträgliche biometrische Fernidentifizierung nicht zu. Übertragene Bilder dürfen nur in Echtzeit, d.h. unmittelbar nach ihrer Fertigung abgeglichen werden. Ein (retrograde) Abgleich Stunden, Tage oder Wochen nach Entstehung wäre unzulässig.

In diesem Zusammenhang muss vorsorglich darauf hingewiesen werden, dass eine nachträgliche biometrische Fernidentifizierung, insbesondere mit Daten aus der Videoüberwachung öffentlichen Raums, aufgrund ihrer Eingriffstiefe und als Hochrisiko-KI-Anwendung selbstverständlich ebenfalls hinreichend bestimmt gesetzlich zu regeln wäre (Art. 6 Abs. 2 i.V.m. Anhang III Nr. 1 Buchst. a der KI-VO) und nicht auf Generalklauseln zur Verarbeitung personenbezogener (biometrischer) Daten zur polizeilichen Aufgabenerfüllung oder auf die die Abgleichsregelung in § 87 SächsPVDG gestützt werden dürfte (vgl. Tätigkeitsbericht der SDTB 2024, S. 26 ff. zur Rechtslage im Bereich der Strafverfolgung; Erwägungsgründe 94 und 95 der KI-VO).

Soweit Abs. 2 Satz 3 vorsieht, die biometrischen Echtzeit-Fernidentifizierung zeitlich und örtlich auf das unbedingt erforderliche Maß zu beschränken, ist aus datenschutzrechtlicher Sicht problematisch, dass im Gesetz nicht näher definiert wird, was unter einer zeitlichen und örtlichen Begrenzung konkret zu verstehen ist. Der Regelung mangelt es (auch) an dieser Stelle an der erforderlichen Bestimmtheit und Verhältnismäßigkeit. Der für richterliche Anordnungen einschlägige § 73 Abs. 3 Satz 3 bestimmt eine Höchstdauer von drei Monaten mit der Option einer Verlängerung nach Satz 4, wobei Satz 5 anordnet, dass u.a. § 57a Abs. 2 Satz 3 unberührt bleiben soll. § 57a Abs. 2 Satz 3 legt allerdings

keine Frist fest, sodass der Wortlaut des Gesetzes sogar eine weitaus längere Anwendung der Maßnahme als drei bzw. sechs Monate erlaubte, wenn dies im Antrag der Polizei und in der richterlichen Anordnung als „unbedingt erforderlich“ angesehen würde. Diese Unschärfe bzw. Unklarheit ist nicht hinnehmbar und muss beseitigt werden.

Gänzlich ungeregt bleibt der Umgang mit „Treffern“, aber auch mit falsch-positiven Ergebnissen des biometrischen Abgleichs. Das Gesetz sieht an anderer Stelle entsprechende Regelungen zur Behandlung von Resultaten automatisierter Datenabgleiche vor (vgl. Abs. 1 Satz 2, § 57 Abs. 9 Satz 3, § 58 Abs. 3 Satz 3 und 4), die hier fehlen. Das ist angesichts der Intensität der Grundrechtseingriffe unverständlich.

Abs. 2 verfehlt daher als gesetzliche Grundlage für die Verarbeitung biometrischer Daten einer sehr großen Zahl von sich rechtstreu verhaltenden Personen, bei denen keinerlei Anhaltspunkte für eine auch nur ansatzweise Gefährlichkeit vorliegen, die verfassungsrechtlich begründeten Anforderungen an Bestimmtheit und Verhältnismäßigkeit.

Soweit Abs. 4 Satz 3 bestimmt, dass das Sächsische Staatsministerium des Innern das Nähere zum Verfahren nach Anhörung der oder des Sächsischen Datenschutz- und Transparenzbeauftragten in einer zu veröffentlichenden Verwaltungsvorschrift zu regeln hat, kann dies die Mängel der Vorschrift des Abs. 2 hinsichtlich der Berücksichtigung der Wesentlichkeitstheorie sowie mit Blick auf Bestimmtheit und Verhältnismäßigkeit nicht heilen. Wesentliche grundrechtserhebliche Entscheidungen können nicht an die Exekutive delegiert werden, sondern sind vom Gesetzgeber zu treffen.

Die in Art. 5 Abs. 2 Satz 3 KI-VO normierten Anforderungen – eine abgeschlossene Grundrechte-Folgenabschätzung und die Registrierung in der entsprechenden EU-Datenbank – finden weder in Abs. 4 noch in der Begründung Erwähnung, obwohl insbesondere die dem Einsatz des Systems vorgelagerte Grundrechte-Folgenabschätzung nach Art. 27 KI-VO für ein rechtsstaatliches Vorgehen elementar ist.

V. Anlassbezogene automatisierte Kennzeichenerkennung - § 58

Die Anpassung der Eingriffsschwellen an die Vorgaben des Bundesverfassungsgerichts und dessen Einordnung der automatisierten Kennzeichenerkennung als eine Maßnahme von erheblichem Eingriffsgewicht ist zu begrüßen.

Dass die Maßnahme künftig auch ohne Wissen der Betroffenen erfolgen darf, ist bedauerlich, aber mit Blick auf die konkret geregelten Anwendungsfälle nachvollziehbar.

Nicht ohne Weiteres nachvollziehbar ist, weshalb stationäre Technik zum Einsatz kommen soll (vgl. Abs. 6), die Anwendungsfälle in Abs. 1 aber durchweg auch in örtlicher Hinsicht „dynamischen Voraussetzungen“ unterliegen. Soweit jeweils vorausgesetzt wird, dass dokumentierte (Abs. 5 Satz 2) „Tatsachen die Annahme rechtfertigen, dass dort Straftaten von erheblicher Bedeutung begangen werden sollen“ (Abs. 1 Nr. 2, 3, 4 und 5) oder eine dokumentierte erhebliche Gefahr vorliegt, enthält dies eine örtliche und zeitliche Komponente, die veränderlich und insofern eher für den Einsatz transportabler Technik sprechen.

Stationäre Technik wird über größere Zeiträume nicht betrieben werden dürfen, wenn keine (aktuellen) Tatsachen dokumentiert sind, die auf die zeitnahe Begehung erheblicher Straftaten am bzw. um den Kontrollort hindeuten.

Abs. 1 Nr. 5 weist zwar einen örtlichen Grenz- bzw. „Transitbezug“ auf, dient aber nicht, wie bislang § 58 Abs. 1 Nr. 4 SächsPVDG, der vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität, sondern soll gänzlich ohne Zweckbestimmung den Einsatz von AKES erlauben, wenn Tatsachen die Annahme rechtfertigen, dass dort zum Zeitpunkt der Kontrolle Straftaten von erheblicher Bedeutung begangen werden sollen. Unter diesen Voraussetzungen dürfte die Kontrolle z. B. von „Verbringungsrouen“ von gestohlenen Fahrzeugen kaum noch möglich sein.

Unklar ist, ob der technikoffen formulierte Abs. 1 den Einsatz sowohl stationärer als auch ambulanter Geräte umfassen soll.

Soll auch der Einsatz transportabler Technik erfasst sein, wäre nicht ersichtlich, aus welchem Grund die in Abs. 6 vorgesehene Evaluierung sich nur auf den stationären Technikeinsatz bezieht. **Die Evaluierung nach Abs. 6 sollte für die Maßnahme generell angeordnet werden, unabhängig davon, ob stationäre oder ambulante Technik zum Einsatz kommt.**

VI. Ausschreibung von Personen und Sachen - § 60

Der Gesetzentwurf gleicht die bislang in § 60 Abs. 2 und 3 bestimmten, unterschiedlichen Voraussetzungen für die verdeckte und die gezielte (offene) Kontrolle an und umfasst auch Ermittlungsanfragen.

Laut Begründung stellt die Ausschreibung zur verdeckten Kontrolle als Maßnahme, die der betroffenen Person nicht bekannt wird, eine eingriffsintensivere Maßnahme als die Ausschreibung zur gezielten Kontrolle oder der Ermittlungsanfrage dar, da letztere der betroffenen Person bekannt werden, weshalb korrekturbedürftig gewesen sei, dass die bisherige Befugnis zur (offenen) gezielten Kontrolle eine höhere Eingriffsschwelle als für die verdeckte Kontrolle vorsah.

Außer Acht bleibt dabei allerdings, dass die Ausschreibung zur gezielten Kontrolle zugleich Voraussetzung für Durchsuchungen nach § 27 Abs. 1 Nr. 6 und § 28 Nr. 1 i.V.m. § 27 Abs. 1 Nr. 6 SächsPVDG ist. Vor diesem Hintergrund sind auch die vermeintlich systemwidrigen Unterschiede der bisherigen Eingriffsschwellen plausibel.

§ 60 Abs. 1 würde also die Voraussetzungen für die Durchsuchung von Personen und Sachen nach §§ 27, 28 absenken. Ein nachvollziehbarer Grund hierfür ist aber nicht ersichtlich und auch nicht im Gesetzentwurf erkennbar.

Vor diesem Hintergrund wäre, soll an § 60 in der Entwurfsfassung festgehalten werden, zwingend § 27 Abs. 1 Nr. 6 SächsPVDG zu ändern, um die Beibehaltung der bisherigen Eingriffsschwelle für Durchsuchungen nach § 27 Abs. 1 Nr. 6 SächsPVDG sicherzustellen.

VII. Elektronische Aufenthaltsüberwachung - § 61

§ 61 enthält nicht nur die Befugnis, eine für eine Gefahr verantwortliche Person zu 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 (Abs. 1), sondern erlaubt der Polizei auch, die automatisiert erhobenen Daten zu einem Bewegungsbild zu verbinden (Abs. 2 Satz 2).

Obwohl die Erstellung eines Bewegungsbildes deutlich eingriffsintensiver ist als die automatisierte „Live-Überwachung“ des Aufenthalts, weil sie auch polizeilich irrelevante, zur Abwehr der Gefahr nicht erforderliche Angaben zum örtlichen Aufenthalt der betroffenen Person fixiert und nachvollziehbar dokumentiert, wird mit der Erforderlichkeit für die Erfüllung des Überwachungszwecks keine andere, höhere Voraussetzung für die Maßnahme bestimmt als für die „Grundanordnung“ nach Abs. 1.

Allein der gesetzlich bestimmte Richtervorbehalt, der freilich für die „Grundanordnung“ ebenso gilt (Abs. 3, 4, 5) wie für die Erstellung eines Bewegungsbildes (Abs. 6), trägt dem Umstand, dass ein Bewegungsbild deutlich tiefer in das Recht der Betroffenen eingreift, nicht in ausreichendem Maß Rechnung.

Die Erstellung eines Bewegungsbildes nach Abs. 2 Satz 2 sollte daher an das Vorliegen von Tatsachen anknüpfen, aufgrund derer anzunehmen ist, dass eine Anordnung nach Abs. 1 zur Erfüllung der Überwachungszwecke nach Abs. 1 nicht ausreichend ist.

VIII. Automatisierte Datenanalyse - § 62a

Der Gesetzentwurf orientiert sich erkennbar an den Vorgaben des Bundesverfassungsgerichts, das in der jüngeren Vergangenheit landesrechtliche Regelungen zur automatisierten Datenanalyse geprüft und dabei den Rahmen skizziert hat, in dem derartige Maßnahmen zulässig sein können (vgl. BVerfG, Urteil vom 16. Februar 2023 - 1 BvR 1547/19 und 1 BvR 2634/20).

Zu beachten ist dabei, dass bereits die Zusammenführung vorhandener – in verschiedenen Zusammenhängen erhobenen und gespeicherten – Daten eine zweckändernde Weiterverarbeitung dieser Daten darstellt. Diesem Umstand wird durch den Verweis auf die Voraussetzungen des § 79a und die Zweckbestimmung (Gewinnung neuer Erkenntnisse) Rechnung getragen.

Zusätzliches Eingriffsgewicht entfaltet die automatisierte Aufbereitung und Auswertung der zusammengeführten Daten (BVerfG, a.a.O., Rn. 69). Dementsprechend ist eine eigenständige Rechtsgrundlage für eine solche Maßnahme erforderlich; diese Funktion soll § 62a erfüllen.

Das Bundesverfassungsgericht stellt fest, dass der Gesetzgeber beim Einsatz von eingriffsintensiven Methoden der Datenauswertung, insbesondere bei komplexen Formen des Datenabgleichs, für schützende Regelungen sorgen muss (BVerfG, a.a.O., Rn. 101).

Maßgeblich sind dabei die zu schützenden Rechtsgüter, die Art der in die Analyse einbezogenen Daten und die Methoden der automatisierten Datenanalyse. Das Bundesverfassungsgericht beschreibt, welche Maßnahmen bzw. Entscheidungen bezüglich dieser Aspekte eingriffserschwerend oder auch eingriffsmindernd wirken können.

Zwar differenziert § 62a durchaus hinsichtlich der Eingriffsschwellen nach verschiedenen Rechtsgütern und Daten, die in die Analyse einbezogen werden können oder aufgrund

besonderer Erhebungsumstände unberücksichtigt bleiben müssen, und unternimmt den Versuch einer Begrenzung des von der Analyse betroffenen Personenkreises. Zur Frage des Verfahrens, das zum Einsatz kommen darf, aber schweigt die Vorschrift.

Dabei wirkt sich die Wahl des Verfahrens durchaus auf die Eingriffsintensität der Maßnahme aus. Das Bundesverfassungsgericht unterscheidet diesbezüglich zwischen „lernfähigen Systemen“, die Muster automatisiert weiterentwickeln oder überhaupt erst generieren und dann in weiteren Analysestufen weiter verknüpfen (BVerfG, a.a.O., Rn. 100), und „deterministischen Systemen“, deren Analysefunktion sich nicht eigenständig verändern kann, sondern in der Software unveränderlich vorprogrammiert ist (BVerfG, a.a.O., Rn. 101).

In diesem Zusammenhang wäre die ausdrückliche gesetzgeberische Festlegung auf den ausschließlichen Einsatz „austrainerter“, deterministischer Systeme eingriffsmindernd und im Hinblick auf die Heterogenität und eventuelle „Polizeifremdheit“ einbezogener Datenquellen geboten. Ein entsprechendes Verbot der Verwendung selbstlernender Systeme – etwa wie in Art. 61a Abs. 5 Nr. 2 BayPAG – würde auch Unklarheiten im Verhältnis zu § 79c vermeiden, der die Verwendung personenbezogener Daten für das Training und Tests von lernenden IT-Systemen regelt. Der Begründung zu § 79c ist zu entnehmen, dass bezweckt wird, „durch Training mit polizeilichen Daten nachvollziehbare Datenverarbeitungsschritte in der jeweiligen (eigen- oder fremdentwickelten) Software unveränderlich zu programmieren und damit die jeweilige spezifische Datenverarbeitung (...) durch austrainerter und ausgelernter Systeme zu ermöglichen“. Dieses Ziel und die in § 79c vorgesehenen grundrechtsschützenden Maßnahmen sollten nicht dadurch unterlaufen werden, dass bei spezifischen Datenverarbeitungsbefugnissen – wie hier § 62a – unklar bleibt, ob lernende Systeme zum Einsatz kommen – und damit zugleich „trainiert“ – werden dürfen.

Verfassungsrechtlich zwingend geboten ist der im Gesetz selbst zu bestimmende **Ausschluss der Verwendung selbstlernender Systeme** jedenfalls bei einer automatisierten Datenanalyse im Vorfeld einer konkretisierten Gefahr (BVerfG a.a.O., Rn. 120, 121), hier also in Fällen des § 62a Abs. 1 Satz 1 Nr. 3. Diese Vorgabe wird in der Vorschrift nicht umgesetzt; der Auftrag an die Exekutive, die Methoden und Techniken, die zur automatisierten Datenanalyse eingesetzt werden dürfen, in einer Verwaltungsvorschrift zu bestimmen (Abs. 4 Satz 1 Nr. 6), genügt den verfassungsrechtlichen Anforderungen nicht.

§ 62a enthält keine Beschränkung der Abgleichmöglichkeiten – damit sind nicht die Vorgaben für die Suche gemeint –, die nach der Entscheidung des Bundesverfassungsgerichts im Gesetz selbst angelegt sein muss (BVerfG a.a.O., Rn 121). Die Vorschrift wäre insoweit zu ergänzen.

Angesichts der Einordnung der automatisierten Datenanalyse als schwerwiegender Eingriff in die informationelle Selbstbestimmung der Betroffenen, der nur unter den engen Voraussetzungen zu rechtfertigen ist, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten (BVerfG, a.a.O., Rn. 104), verwundert es, dass § 62a weder einen **Richtervorbehalt** noch eine **Benachrichtigungspflicht** vorsieht, die für eingriffsintensive heimliche Überwachungsmaßnahmen Standard sind. Insbesondere wenn externe Datenbestände in die Analyse einbezogen werden, ist nicht nachvollziehbar, weshalb Betroffene hinsichtlich einer vorgelagerten unabhängigen Kontrolle und einer nachgelagerten Information weniger schutzwürdig sein sollen als die in § 74 Abs. 1

genannten Personen. **Jedenfalls für diese Fälle wäre eine nachträgliche Benachrichtigungspflicht in § 74 Abs. 1 SächsPVDG aufzunehmen.**

Unklar bleibt in der Vorschrift auch, wie **nach Abschluss der Maßnahme** mit den zusammengeführten und analysierten Daten auf der Analyseplattform verfahren werden soll, die nicht als neue Erkenntnisse in den konkreten und für die Durchführung der Maßnahme ursächlichen Vorgang übernommen werden. Eine diesbezügliche Regelung wäre aber dringend notwendig, weil § 62a auch die Einbeziehung externer Datenbestände – aus behördlichen ebenso wie nicht-öffentlichen Datenbeständen – erlauben soll, die der Polizei zum Zeitpunkt der Anordnung der Maßnahme gerade nicht vorliegen (Abs. 3 Satz 2). Diese Daten sollen, so die Zweckbestimmung der Vorschrift, lediglich der (erhofften) Gewinnung neuer Erkenntnisse dienen. Für eine mittel- oder gar längerfristige Übernahme dieser Daten in den polizeilichen Datenbestand ist dies keine verfassungsrechtlich hinreichende Rechtfertigung. **Insofern wäre die Anordnung einer Löschung der Daten in der Analyseplattform nach Abschluss der Maßnahme dringend geboten.**

Abs. 1

Dass die Zweckbestimmung und die Festlegung verschiedener der Eingriffsschwellen in **§ 62a Abs. 1** sowohl die Zusammenführung von Daten als auch deren automatisierte Auswertung erfasst, ist nicht zu beanstanden.

Unverständlich ist, aus welchem Grund in der Aufzählung der gefährdeten Rechtsgüter in Satz 1 Nr. 3 sowohl „Leib“ als auch „Gesundheit“ auftauchen. Da das Rechtsgut „Leben“ gesondert aufgeführt wird, kann es sich bei einer Gefahr für „Leib“ oder „Gesundheit“ nur um ein und dieselbe Gefahr handeln. Hier wäre entweder „Leib“ oder „Gesundheit“ zu streichen.

Hinsichtlich der in **Satz 1 Nr. 3** beschriebenen Gefährdungslagen ist anzumerken, dass Konstellationen weit im Vorfeld einer konkreten Rechtsgutgefährdung vorliegen, wie auch die Begründung einräumt. Die Regelung verweist u.a. auf die Norm des § 100a Absatz 2 StPO, die derzeit defekt ist und auf Straftatbestände verweist, die lediglich eine Höchstfreiheitsstrafe von drei Jahren oder weniger vorsehen und damit dem einfachen Kriminalitätsbereich zuzuordnen sind (BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 215, juris). Die gebotene Begrenzung auf mindestens schwere Straftaten, die wegen der fehlenden Konkretisierung der Gefahr erforderlich ist, wird damit verfehlt. Dieser Defekt kann auch nicht durch Abs. 1 Satz 3 geheilt werden, der laut Begründung sicherstellen soll, dass die zu verhütende Straftat auch im Einzelfall schwer wiegt. Eine solche Regelungsanordnung kann Satz 3 dem Wortlaut nach gerade nicht entnommen werden: „Im Fall einer Straftat nach § 100a Absatz 2 der Strafprozessordnung muss die zu verhütende Straftat auch im Einzelfall vorliegen“. Der Satz ist unverständlich und trifft keine Aussage über die Schwere der jeweiligen Straftat.

Ausdrücklich ist noch einmal auf die Unzulässigkeit der Verwendung selbstlernender Systeme jedenfalls bei einer automatisierten Datenanalyse im Vorfeld einer konkretisierten Gefahr hinzuweisen (s.o.).

Abs. 2

Nach Abs. Satz 2 soll bei der automatisierten Datenanalyse sicherzustellen sein, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Die Verwendung des Begriffs des „Herausbildens“ und der in der Begründung enthaltene Hinweis auf Rn. 100 der Entscheidung des Bundesverfassungsgerichts vom 16. Februar 2023 legen nahe, dass in der Regelung vom Einsatz selbstlernender Systeme ausgegangen wird, die in Rn. 100 thematisiert werden.

Allerdings ist der regelmäßige und alle Anwendungsfälle erfassende Einsatz solcher Systeme im Rahmen von § 62a gerade keine Selbstverständlichkeit und wäre im Hinblick auf das weite (technische) Spektrum möglicher automatisierter Auswertungsverfahren, das auch das Bundesverfassungsgericht in den Blick nimmt (BVerfG a.a.O., Rn. 100, 101, 108), äußerst problematisch bzw. klar unzulässig (s.o. zu Abs. 1 Nr. 3).

Wie oben erwähnt, wäre vor dem Hintergrund der Regelung des § 79c und der Erforderlichkeit von eingriffsmindernden Maßnahmen bei der automatisierten Datenanalyse ein **Verbot der Verwendung selbstlernender Systeme geboten**, wodurch nur rechtmäßig austrainierte und unveränderliche KI-Systeme zum Einsatz kommen könnten.

Abs. 3

Absatz 3 beschreibt den Umfang bzw. die Art der Daten, die in eine automatisierte Datenanalyse einbezogen werden dürfen.

Satz 1 ist eher eine Beschreibung des kompletten Datenbestandes der Polizei als eine – so die Begründung – eingriffsmindernde Begrenzung, da fast ausnahmslos sämtliche der Polizei vorliegende Daten erfasst werden. Zutreffend wird in der Begründung dann auch darauf hingewiesen, dass die Daten aus der Vorgangsverwaltung gemäß § 79 Absatz 2 SächsPVDG von besonderer praktischer Bedeutung seien, wobei ein Vorgang sämtliche Unterlagen umfasst, die im Zusammenhang mit einer polizeilichen Tätigkeit über eine bestimmte Person, Sache oder sonstigen Gegenstand polizeilichen Handelns geführt werden. Aufgenommen würden insbesondere Anzeigen, Ermittlungsberichte und Vermerke, die nicht nur Daten zu Verdächtigen, Beschuldigten oder sonstigen Anlasspersonen enthalten, sondern beispielsweise auch zu Personen, die Anzeige erstatten, Hinweise geben oder Zeuginnen oder Zeugen sind.

Dem (fehlgeschlagenen) Versuch einer Begrenzung von polizeilichen Datenbeständen in Satz 1 folgt in Satz 2 mit der Möglichkeit der Einbeziehung von polizeifremden Daten aus staatlichen Registern oder aus gesondert gespeicherten Daten aus Internetquellen eine weitgehende Entgrenzung der Datenbestände, die nach § 62a analysiert werden dürfen. Damit ist eine deutliche Vertiefung des Eingriffsgewichts der Maßnahme verbunden.

Völlig unklar ist, ob und gegebenenfalls wie Satz 3 technisch umgesetzt werden kann, der bestimmt, personenbezogene Vorgangsdaten zu Unbeteiligten von der automatisierten Datenanalyse auszunehmen. Grundlegend ist laut Begründung zu Abs. 4 „die Unterscheidung zwischen einerseits unbeteiligten und andererseits verurteilten, beschuldigten und verdächtigen Personen sowie sonstigen Anlasspersonen und deren Kontaktpersonen (siehe § 28 SächsDSUG)“. Eine solche Maßnahme würde das Eingriffsgewicht der Maßnahme hinsichtlich ihrer Streubreite und der Zahl von Mitbetroffenen zweifellos deutlich reduzieren und wäre insoweit ausdrücklich zu begrüßen. Es stellt sich allerdings die

Frage, ob die Anordnung überhaupt befolgt werden kann oder zur faktischen Unanwendbarkeit einer automatisierten Datenanalyse nach § 62a Abs. 1 führt:

In Fällen von Abs. 1 Satz 1 Nr. 1 knüpft die Maßnahme an das Vorliegen einer Gefahr für ein gewichtiges Rechtsgut an, wobei nicht immer bekannt sein dürfte, ob es beteiligte und unbeteiligte bzw. für die Gefahr verantwortliche oder nicht verantwortliche Personen gibt und wer genau diese Personen sind. Damit gäbe es, wollte man nicht von einer nahezu unbegrenzten Zahl von „Beteiligten“ ausgehen, nur „Unbeteiligte“ im Sinne von Satz 3, deren Daten aus Vorgangsdaten nicht für eine automatisierte Datenanalyse genutzt werden dürfen. In den Fällen von Abs. 1 Satz 1 Nr. 2 und 3 geht der Entwurf von einer Zuordnung der Gefährdungslagen zu konkreten, der Polizei bekannten Personen aus, wie Abs. 2 Satz 3 zeigt, wonach „der Suchvorgang auf die nach den §§ 6 und 7 Verantwortlichen auszurichten“ ist. In der Regel dürften zu diesen Personen polizeiliche Datenbestände vorliegen. Wenn aber Vorgangsdaten als eine der wichtigsten Datenquellen in die Analyse einbezogen werden (Abs. 3 Satz 1) und diese Vorgangsdaten „nicht nur Daten zu Verdächtigen, Beschuldigten oder sonstigen Anlasspersonen enthalten, sondern beispielsweise auch zu Personen, die Anzeige erstatten, Hinweise geben oder Zeuginnen oder Zeugen sind“ (Begründung) – hinzu treten ggf. Daten zu Geschädigten und Bezugspersonen –, dann müssen Vorgangsdaten vor einer Einbeziehung in eine automatisierte Datenanalyse umfangreich „sortiert“ werden, um Daten „Unbeteiligter“, d.h. nicht nach §§ 6 und 7 Verantwortlicher, auszusondern.

Wenn die Umsetzung der Anordnung von Abs. 3 Satz 3 technisch gelänge, würden datenschutzrechtliche Bedenken gegen die automatisierte Datenanalyse erheblich geringer ausfallen.

Voraussetzung dafür ist, wie auch in der Entwurfsbegründung anklingt, eine zuverlässige Kennzeichnung personenbezogener Daten in der polizeilichen Vorgangsbearbeitung ebenso wie in der übrigen polizeilichen Datenhaltung. Kennzeichnungen, die Unterscheidungen nach Kategorien von Personen (vgl. § 28 SächsDSUG), nach Tatsachen und persönlichen Einschätzungen (vgl. § 29 SächsDSUG) und nach Eingriffsgewicht der ursprünglichen Erhebungsmaßnahme sowie Schwere des Erhebungsanlasses (vgl. § 81 Abs. 1 Nr. 1 und Nr. 3 SächsPVDG) ermöglichen, verringern das Risiko von erheblichen Eingriffen in Rechte Unbeteiligter und sind – jedenfalls bezüglich der Informationen zur ursprünglichen Datenerhebung – Voraussetzung für die Erfüllung der Anforderungen, die § 79a Abs. 2 in Umsetzung des Prinzips der hypothetischen Datenneuerhebung an die zweckändernde Weiterverwendung personenbezogener Daten stellt. Das nur aufgrund einer funktionierenden Kennzeichnung funktionierende Filtern sehr großer Datenbestände ist eine *Conditio sine qua non* für die rechtmäßige Anwendung einer automatisierten Datenanalyse.

Die Begründung zu Abs. 4 lässt eine gewisse Skepsis der Verfasser erkennen, was die zeitnahe Etablierung einer Kennzeichnungspraxis betrifft, die die Beachtung und Befolgung von § 79a Abs. 2, aber auch von den in § 62a Abs. 2 Satz 4 und Abs. 3 Satz 3 und 4 formulierten eingriffsmindernden Anordnungen ermöglicht. Völlig zutreffend wird auf die negative Wirkung von § 81 Abs. 4 SächsPVDG hingewiesen, der die in § 81 Abs. 1 bis 3 SächsPVDG getroffenen Anordnungen weitestgehend entwertet.

Während dieser Umstand bei einzelnen, „händischen“ zweckändernden Weiterverarbeitungen personenbezogener Daten keine gravierenden Auswirkungen hat, weil die Voraussetzungen etwa von § 79 Abs. 2 SächsPVDG (künftig § 79a Abs. 2) „händisch“ und mit überschaubarem Aufwand geprüft werden können, ist eine solche Prüfung bei der

Zusammenführung von Einbeziehung von Vorgangsdaten, Falldaten, Daten aus polizeilichen Auskunftssystemen, Verkehrsdaten, Daten aus Asservaten und Daten aus dem polizeilichen Informationsaustausch zum Zweck der automatisierten Auswertung praktisch unmöglich, wenn die Daten zeitnah auf der Analyseplattform zur Verfügung stehen sollen.

Abs. 3 Satz 5 ordnet die Löschung von zur Datenanalyse gespeicherten personenbezogenen Verkehrsdaten nach zwei Jahren an. Ungeregelt bleibt, wie oben erwähnt, der Umgang mit anderen personenbezogenen Daten, die für die automatisierte Datenanalyse zusammengeführt (im Fall von externen Registerdaten und Daten aus dem Internet sogar erstmals erhoben) wurden und aus denen sich keine neuen Erkenntnisse zur Sachverhaltsaufklärungen ergeben haben. Eine doppelte Speicherung polizeilicher Daten im originären Speicherzusammenhang einerseits und auf der Analyseplattform andererseits birgt das Risiko der Umgehung der für die originäre Datenhaltung geltenden Speicherfristen; hinsichtlich der allein für die automatisierte Datenanalyse hinzugezogenen polizeifremden Daten (Abs. 3 Satz 2) ist eine Rechtfertigung für die Aufbewahrung über die automatisierte Analyse hinaus gar nicht ersichtlich.

Vor diesem Hintergrund sollte bestimmt werden, dass die nach Abs. 3 Satz 1 und 2 zusammengeführten bzw. erhobenen Daten nach Abschluss der automatisierten Datenanalyse zu löschen sind, soweit sie nicht neue Erkenntnisse für die Erfüllung des jeweiligen Zwecks nach Abs. 1 Satz 1 belegen.

Zu Abs. **4 Satz 1 Nr. 6** ist anzumerken, dass, wie bereits erwähnt, gesetzlich bestimmt werden sollte, dass bei der automatisierten Datenanalyse der Einsatz selbstlernender Systeme unzulässig ist (s.o., vgl. Art. 61a Abs. 5 Nr. 2 BayPAG). Hinsichtlich der automatisierten Datenanalyse im Vorfeld einer konkretisierten Gefahr – hier also im Fall von Abs. 1 Satz 1 Nr. 3 – wäre ein solches Verbot ohnehin zwingend gesetzlich festzulegen (s.o., BVerfG a.a.O., Rn. 120).

Nach Abs. 4 Satz 1 Nr. 7 sollen in einer Verwaltungsvorschrift „verfahrensrechtliche Maßnahmen“ zum Zweck der Erkennung und Korrektur fehlerhafter Datenauswertung bestimmt werden. Hier irritiert die Verwendung des Begriffs der „verfahrensrechtlichen Maßnahmen“; es ist nicht ersichtlich, in welchem rechtlich formalisierten Verfahren sich ein Monitoring der Entwicklung der eingesetzten Software – vermutlich knüpft die Regelung an die Feststellung des Bundesverfassungsgerichts in Rn. 109 der Entscheidung vom 16. Februar 2023 an – bewegte.

§ 62a verfehlt an verschiedenen Stellen grundlegende verfassungsrechtliche Anforderungen und ist stark überarbeitungsbedürftig.

IX. Biometrischer Abgleich mit Daten aus dem Internet - § 62b

Die Vorschrift soll der Polizei erstmals ermöglichen, im öffentlich zugänglichen Internet Personen anhand von Bildern oder Stimmen automatisiert zu identifizieren. Die Befugnis stellt einen erheblichen Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung dar und erfasst Personen, deren Abbildungen und akustische Äußerungen im Internet zugänglich sind, in öffentlichen und in privaten Bereichen sowohl gezielt als auch ungezielt.

Damit wird der gesamte öffentlich zugängliche Bereich des Internets praktisch zu einer Referenzdatenbank für polizeiliche Maßnahmen, mindestens Millionen von Menschen müssen dauerhaft gewärtigen, einem biometrischen Abgleich hinsichtlich ihrer im Internet zugänglichen Bilder und Tonaufzeichnungen mit polizeilichen Referenzdaten unterzogen zu werden. Die Streubreite der Maßnahme ist enorm.

Zutreffend weist die Begründung darauf hin, dass es sich beim automatisierten biometrischen Abgleich mit Daten aus dem Internet um eine Maßnahme handelt, die von der Eingriffsintensität heimlichen eingriffsintensiven Überwachungsmaßnahmen gleichkommt. Damit dieser Eingriff in das Grundrecht auf informationelle Selbstbestimmung den Grundsätzen der Verhältnismäßigkeit genügt, gelten daher als Maßstab für die verfassungsgemäße Ausgestaltung einer gesetzlichen Regelung die Anforderungen des Bundesverfassungsgerichts für die Ausgestaltung von heimlichen Überwachungsmaßnahmen (siehe BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 und 1 BvR 1140/09, Rz. 103 ff, 117ff). Im Bereich der Gefahrenabwehr setze dies das Vorliegen einer konkreten Gefahr für ein überragend wichtiges Rechtsgut voraus. Überragend wichtig seien Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt (BVerfG, a. a. O., Rz. 108).

Benennt der Gesetzgeber das zu schützende Rechtsgut nicht unmittelbar, sondern knüpft er an Straftatbestände an, müssen diese entsprechend schwer wiegen. Dem verfassungsrechtlichen Erfordernis eines besonders gewichtigen Rechtsguts entspricht jedenfalls eine Begrenzung auf besonders schwere Straftaten im verfassungsrechtlichen Sinn, also zunächst solche, die mit einer Höchstfreiheitsstrafe von mehr als fünf Jahren bedroht sind (BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 2466/19 –, Rn. 137, juris).

Laut Entwurfsbegründung setzt die Eingriffsschwelle in **Abs. 1 Satz 2 Nummer 1** das Vorliegen einer konkretisierten Gefahr durch die Verhütung von schweren Straftaten voraus. Die Schwere der Straftat soll vermutlich durch den Verweis auf den Katalog von § 100a Abs. 2 StPO sichergestellt werden. Die Vorschrift des § 100a Absatz 2 StPO ist derzeit allerdings defekt (in Teilen ist die Vorschrift nichtig: BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 180/23) und verweist auch auf Straftatbestände, die lediglich eine Höchstfreiheitsstrafe von drei Jahren oder weniger vorsehen und damit dem einfachen Kriminalitätsbereich zuzuordnen sind (BVerfG a.a.O., Rn. 215, juris). Die laut Begründung von den Verfassern intendierte Begrenzung auf die Verhütung mindestens schwerer Straftaten wird damit verfehlt.

Der Gesetzgeber kann im präventiven Bereich den erforderlichen Rechtsgüterschutz aber unabhängig vom Gewicht der Straftat mit einer ergänzenden Rechtsgutbetrachtung sicherstellen (BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 2466/19 –, Rn. 138, juris). Folgt die unmittelbare Ausrichtung am Schutz qualifizierter Rechtsgüter nicht schon aus der Strafnorm selbst, kann der erforderliche Rechtsgüterschutz auch dadurch sichergestellt werden, dass der Gesetzgeber die in einer polizeilichen Befugnisnorm in Bezug genommenen Straftatbestände dahingehend näher qualifiziert, dass sie im Einzelfall dem Schutz entsprechender Rechtsgüter dienen müssen (vgl. BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 2466/19 –, Rn. 138, juris).

Dem sächsischen Gesetzgeber ist eine solche Regelungstechnik vertraut; in § 66 Abs. 1 Satz 2 Nr. 2 SächsPVDG findet sich bereits eine entsprechende Bestimmung.

Abs. 1 Satz 2 Nummer 1 sollte daher um eine Rechtsgutbetrachtung ergänzt werden, die den erwähnten verfassungsrechtlichen Anforderungen genügt.

Datenschutzrechtlich problematisch ist die Fehleranfälligkeit von Systemen zur automatisierten Fernidentifizierung. Selbst bei einer außerordentlich geringen Fehlerquote wäre aufgrund der großen Menge an erfassten Personen die Zahl der von falsch-positiven Treffern sehr hoch, womit eine nicht geringe Wahrscheinlichkeit dafür anzunehmen ist, dass Personen aufgrund von automatisierten Falschbewertungen zu Unrecht eingriffsstarken polizeilichen Maßnahmen unterworfen werden können.

Äußerst kritisch sind – sowohl in verfassungsrechtlicher als auch in polizeifachlicher Hinsicht – auch Diskriminierungstendenzen bei Verfahren der automatisierten biometrischen Gesichtserkennung zu betrachten.

Es wäre bereits im Gesetz selbst sicherzustellen, dass ausschließlich rechtmäßig austrainierte, unveränderliche und diskriminierungsfreie Systeme zum Einsatz kommen (vgl. VIII. zu § 62a Abs. 2 Satz 2, XVIII. zu § 79c Abs. 1 Satz 2).

X. Einsatz einer V-Person - § 64

Derzeit wird die Verfassungsmäßigkeit der Vorschrift des § 64 Abs. 1 durch das Bundesverfassungsgericht überprüft (1 BvR 2817/20).

Unter rechtsstaatlichen Gesichtspunkten ist es notwendig, dass der Staat, wenn er sich zur Erfüllung seiner (hoheitlichen) Aufgaben Personen bedient, die keine Amtsträger sind, bei der Auswahl dieser Personen sorgfältig vorgeht und darauf achtet, dass sie nicht völlig ungeeignet sind und/oder in ihren Handlungen massiv gegen die Rechtsordnung verstoßen. Dem Einsatz von V-Personen wohnt insoweit ein hohes Risiko inne.

Weil die personenbezogenen Daten beim Einsatz von V-Personen (zunächst) gerade nicht von Amtsträgern erhoben oder „eingeholt“ werden, sodass mitunter schwerwiegende polizeiliche Grundrechtseingriffe in Handlungen externer Personen ihren Anfang nehmen, ist der Gesetzgeber mit Blick auf die Wesentlichkeitstheorie gehalten, den Kreis potentieller V-Personen zu begrenzen. Dies gilt insbesondere vor dem Hintergrund, dass Informationen von V-Personen unmittelbar zu operativen (Zwangs-)Maßnahmen gegen betroffene Personen führen können.

Als Vorschrift zur Auswahl von V-Personen ungeeignet bzw. unzureichend sind § 64 Abs. 5 und 6 zu bewerten. Vor einem Einsatz als V-Person sollen demnach lediglich Minderjährigkeit und Betreuungsbedürftigkeit sowie das Vorliegen von Zeugnisverweigerungsrechten zu berücksichtigen sein und zu einem Ausschluss des Einsatzes führen (§ 64 Abs. 5 SächsPVDG). Andere zum Teil sehr vage formulierte Gründe – etwa „Ungeeignetheit“ nach § 64 Abs. 6 Nr. 2 SächsPVDG –, die gegen einen Einsatz als V-Person sprechen, sollen nach § 64 Abs. 6 SächsPVDG lediglich bzw. erst zur Beendigung der Zusammenarbeit führen.

Vor dem Hintergrund rechtsstaatlich hochproblematischer Erfahrungen mit V-Personen und dem Bestreben der Innenministerkonferenz, den V-Personen-Einsatz auf dem Gebiet des Verfassungsschutzes zu standardisieren (<https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/13-12-06/Anlage3.pdf?blob=publicationFile&v=3>) haben der Bundesgesetzgeber wie auch der sächsische Gesetzgeber Vorschriften zur Auswahl und zum Einsatz von V-Personen

in das jeweilige Verfassungsschutzgesetz aufgenommen (§ 9b Abs. 2 Satz 1 BVerfSchG, § 12 Abs. 2 Satz 1 SächsVSG). Die Intensität des Grundrechtseingriffs beim Einsatz von V-Personen durch Verfassungsschutzbehörden ist vergleichbar mit derjenigen beim Einsatz von V-Personen durch Polizeibehörden; in beiden Fällen handelt es sich um eine verdeckte Maßnahme unter Ausnutzung eines Vertrauensverhältnisses. Beim polizeilichen Einsatz von V-Personen kommt allerdings erschwerend hinzu, dass Informationen von V-Personen direkt für operative Anschlussmaßnahmen der Polizei genutzt werden können.

Vor diesem Hintergrund sollte § 64 Abs. 5 an § 12 Abs. 2 SächsVSG angepasst werden; die Kriterien nach § 12 Abs. 2 Satz 1 SächsVSG sollten in den Wortlaut von Abs. 5 übernommen werden.

XI. Quellen-TKÜ - § 66 Abs. 2, 2a

Die neue Befugnis zur Quellen-Telekommunikationsüberwachung begründet Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-System-Grundrecht) sowie in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis (BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 172, juris).

Das Bundesverfassungsgericht erläutert anschaulich, aus welchen Gründen die Quellen-TKÜ einen besonders schweren Eingriff in Rechte der Betroffenen darstellt:

Art und Umfang der erhobenen Daten wirken schon für sich genommen eingriffsverstärkend, denn die Quellen-Telekommunikationsüberwachung ermöglicht Ermittlungsbehörden den Zugang zu einem Datenbestand, der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei weitem übertreffen kann (BVerfG a.a.O., Rn. 187, juris).

Die Überwachung und Aufzeichnung der laufenden Telekommunikation in Form der Quellen-TKÜ umfasst – nach der maßgeblichen materiellen Betrachtung der von dieser Befugnis eröffneten rechtlichen und tatsächlichen Nutzungsmöglichkeiten – die Ausleitung des gesamten Rohdatenstroms. Dieser kann – anders als bei der klassischen Telekommunikationsüberwachung – trotz einer etwaigen Verschlüsselung vollständig ausgewertet werden; alle Daten des ausgeleiteten Rohdatenstroms sind für die Behörden lesbar. Die Befugnis hat damit insbesondere unter den heutigen Bedingungen der Informationstechnik und ihrer Bedeutung für die Kommunikationsbeziehungen eine außerordentliche Reichweite. So wird mit den erfassten Datenströmen nicht nur eine unübersehbare Zahl von Formen elektronischer Kommunikation transportiert und der Auswertung zugeführt. Angesichts der ubiquitären und vielfältigen Nutzung von IT-Systemen findet inzwischen auch zunehmend jede Art individuellen Handelns und zwischenmenschlicher Kommunikation in elektronischen Signalen ihren Niederschlag und wird so insbesondere der Quellen-Telekommunikationsüberwachung zugänglich. Die Überwachung erfasst damit auch tief in den Alltag hineinreichende, auch höchst private und spontane Kommunikationsvorgänge einschließlich gespeicherter Bilder und Dokumente (vgl. BVerfG a.a.O., Rn. 188, juris).

Eingriffsverstärkend wirkt auch, dass eine Quellen-Telekommunikationsüberwachung nicht nur heimlich erfolgt, sondern mit dem Zugriff auf ein IT-System gezielt Sicherungsmechanismen wie insbesondere der Einsatz von Verschlüsselungstechnologie umgan-

gen werden. Die Vereitelung solchen informationellen Selbstschutzes erhöht das Gewicht der Grundrechtseingriffe. Mit dem Zugriff auf das IT-System werden zudem berechnete Erwartungen in dessen Integrität und Vertraulichkeit beeinträchtigt. Verbunden ist damit ein hohes Gefährdungspotential. Einmal in das IT-System eingedrungen, ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems überwunden (BVerfG a.a.O., Rn. 192, juris).

Schon mit dem Zugriff als solchem geht das Risiko einer funktionellen Beeinträchtigung des IT-Systems einher. Dabei ist zu beachten, dass es einen rein lesenden Zugriff jedenfalls bei Infiltration eines IT-Systems mit einer Überwachungssoftware nicht gibt. Sowohl die Ermittlungsbehörde als auch von ihr mit der Durchführung betraute Dritte können Datenbestände versehentlich oder durch gezielte Manipulationen löschen, verändern oder neu anlegen. Zu berücksichtigen sind auch die mit dem Zugriff auf ein IT-System mittelbar einhergehenden Gefährdungen. Denn Ermittlungsbehörden dürfen insbesondere mit einer Überwachungssoftware auf ein Zielsystem zugreifen und dafür unbekannte IT-Sicherheitslücken ausnutzen (sog. Zero-Day-Exploits). So wirkt sich auf das Eingriffsgewicht aus, dass schon die Existenz dieser Befugnis einen Anreiz für Ermittlungsbehörden schafft, ihnen bekannte Sicherheitslücken offenzuhalten, um sie für eine Infiltration nutzen zu können. In der Folge besteht die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sie sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben (BVerfG a.a.O., Rn. 194, juris).

Die Quellen-Telekommunikationsüberwachung ermöglicht den Zugriff auf von einer betroffenen Person genutzte IT-Systeme in ihrer ganzen Breite. Polizeibehörden dürfen mit technischen Mitteln dergestalt auf IT-Systeme zugreifen, dass deren Leistungen, Funktionen und Speicherinhalte potenziell genutzt werden können. Unerheblich ist dabei, dass die Überwachung und Aufzeichnung auf die laufende Telekommunikation begrenzt ist. Denn diese Begrenzung lässt unberührt, dass das Gefährdungspotenzial, das mit der Nutzung technischer Mittel unmittelbar einhergeht, auf die Vertraulichkeitserwartung an das IT-System insgesamt bezogen ist. Einmal in das System eingedrungen, ist die Vertraulichkeit aller dort erzeugter, verarbeiteter und gespeicherter oder von dort aus zugänglicher Daten erheblich gefährdet (BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 2466/19 –, Rn. 103, juris).

Angesichts dieser Äußerungen und Feststellungen des Bundesverfassungsgerichts ist unverständlich, weshalb in der Begründung zu Abs. 2 ausgeführt wird, dass die Quellen-TKÜ als besondere Form der Telekommunikationsüberwachung (lediglich) an Artikel 10 Absatz 1 GG (Art. 27 Abs. 2 SächsVerf) zu messen sei und nur die Kommunikation erfasse, die auch durch eine konventionelle TKÜ erlangt würde. Das ist offensichtlich unzutreffend, der Eingriff betrifft tatsächlich zwei Grundrechte und wiegt wesentlich schwerer als die konventionelle TKÜ, mit der kein zusätzlicher Eingriff in das IT-Grundrecht verbunden ist.

Datenschutzrechtlich besonders kritisch ist die staatliche Nutzung von (allgemein) unbekannten Schwachstellen in Softwareprogrammen. Relevant ist dieser Umstand im Hinblick auf die Eröffnung des Schutzbereichs des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (s.o.). Den Staat trifft insofern eine Schutzpflicht für die IT-Sicherheit.

Es ist dem Staat zwar erlaubt, für den Erfolg polizeilicher Maßnahmen alle verhältnismäßigen und erlaubten Mittel einzusetzen. Es ist ihm allerdings nicht erlaubt, bekannte Sicherheitslücken für den Erfolg verdeckter Maßnahmen bewusst bestehen zu lassen, wenn davon der Schutz des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aller anderen, unbescholtenen Nutzer betroffen ist.

Die Ausnutzung einer Schwachstelle durch den Staat ist nur dann verhältnismäßig, wenn der Staat gleichzeitig den Hersteller über die Schwachstelle informiert, so dass diese geschlossen werden kann.

Insofern sollte Abs. 3 dahingehend ergänzt werden, dass Schwachstellen in Programmsystemen, die deren Herstellern noch nicht bekannt sind, nur ausgenutzt werden dürfen, wenn die Schwachstellen unverzüglich den Herstellern gemeldet werden.

In jedem Fall ist beim Offenhalten einer Sicherheitslücke eine **Datenschutz-Folgenabschätzung** vorzunehmen (vgl. BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 2466/19, Rn. 53, juris; BVerfG, Beschluss vom 9. Dezember 2022 – 1 BvR 1345/21, Rn. 67).

XII. Erhebung von Bestandsdaten - § 70

§ 70 Abs. 1 Satz 2 Nr. 2 Buchst. d soll die Erhebung von Passwörtern und Zugangsdaten nach § 23 Absatz 2 Nummer 2 TDDDG erlauben, wenn dies erforderlich ist zur Abwehr einer konkreten Gefahr für die „freiheitlich demokratische Grundordnung“.

Die freiheitliche demokratische Grundordnung als Begriff, der jene zentralen Grundprinzipien umfasst, die für den freiheitlichen Verfassungsstaat schlechthin unentbehrlich sind (BVerfG, Urteil vom 17. Januar 2017 – 2 BvB 1/13 –, BVerfGE 144, 20-369 (LT 1-9)), ist in seiner Weite und fehlenden Konkretheit ungeeignet, als Rechtsgut im polizeirechtlichen Sinn angesehen zu werden, zu dessen Schutz Grundrechtseingriffe durch den Polizeivollzugsdienst legitimiert werden können.

Die freiheitliche demokratische Grundordnung wird lediglich in § 2 Abs. 1 Satz 2 SächsPVDG im Rahmen der allgemeinen Aufgabenbeschreibung des Polizeivollzugsdienstes erwähnt, im Übrigen an keiner Stelle des Gesetzes, insbesondere nicht im Wortlaut der Vorschriften zu konkreten polizeilichen Befugnissen, die Grundrechtseingriffe zum Schutz bestimmter Rechtsgüter erlauben. Die verfassungsgerichtliche Rechtsprechung bezieht sich – soweit ersichtlich – auch in keiner Entscheidung zu polizeilichen Eingriffsbefugnissen und zur Kategorisierung von Rechtsgütern auf die freiheitliche demokratische Grundordnung.

Vor diesem Hintergrund, vor allem aber mit Blick auf die fehlende Bestimmtheit des Begriffs sollte § 70 Abs. 1 Satz 2 Nr. 2 Buchst. d ersatzlos gestrichen werden.

XIII. Einsatz von Drohnen bei Datenerhebungen - § 71

Die Vorschrift stellt hinsichtlich bestimmter, technikoffener Datenerhebungsbefugnisse klar, dass die jeweilige Datenerhebung auch mittels Einsatzes von Drohnen erfolgen kann.

Zutreffend weist die Begründung darauf hin, dass mit der Regelung keine Befugnisweiterung verbunden ist. Ausdrücklich zu begrüßen ist in diesem Zusammenhang Abs. 2, wonach im Fall der richterlichen Anordnung einer Datenerhebung die Anordnung auch den Einsatz von Drohnen erfassen muss. Dies trägt dem Umstand Rechnung, dass eine Datenerhebung mittels Drohne potentiell eingriffsintensiver ist als eine konventionelle offene Erhebung auf Erdbodenniveau, da sie je nach Umständen für Betroffene schwerer bis kaum zu erkennen ist.

Völlig unverständlich ist insofern, auf welcher verfassungsrechtlichen Grundlage in der Begründung davon ausgegangen wird, dass im Fall von Gefahr im Verzug von der Offenheit der Maßnahme auch dann abgesehen werden könne, wenn die grundlegende Datenerhebungsbefugnis, die die Erhebung (nur) als offene Maßnahme zulässt, Ausnahmen von der Offenheit gerade nicht – auch nicht bei Gefahr im Verzug – zulässt.

§ 71 darf nicht dazu führen, dass die gesetzlichen Anforderungen an die Offenheit der Maßnahme durch äußere und technische Rahmenbedingungen umgangen werden. Nur weil die gesetzlich geforderte Offenheit der Maßnahme beim Einsatz von Drohnen möglicherweise technisch und tatsächlich schwer umzusetzen ist, darf aus einer offenen Maßnahme keine faktisch verdeckte Maßnahme der Datenerhebung werden. Dies gilt für alle Datenerhebungen nach §§ 56 und 57 Abs. 1 bis 3 und 9.

Am Beispiel von § 57 Abs. 3 Nr. 2 – offene Videoüberwachung von Kriminalitätsschwerpunkten – wird angesichts dessen, dass derartige Maßnahmen in der Praxis seit Jahrzehnten mit der Information potentiell Betroffener durch Hinweisschilder verbunden sind, die für die präventive Wirkung der Maßnahme elementar sind, deutlich, dass der Einsatz von schwer erkennbaren Drohnen nicht nur das Risiko birgt, wegen mangelnder Offenheit rechtswidrig zu sein, sondern auch die präventive Zweckbestimmung der „Grundmaßnahme“ verfehlt.

Insbesondere für Datenerhebungen nach § 57 Abs. 3 und 9, die nicht an das Verhalten von Personen anknüpfen, sondern gewissermaßen „stationär“ an die abstrakte Gefährlichkeit bestimmter Örtlichkeiten, sollte daher der Einsatz von Drohnen gesetzlich ausgeschlossen werden.

Offene Datenerhebungen bei Versammlungen nach § 11 Abs. 1 und 2 SächsVersG, die ausschließlich der Polizeivollzugsdienst vornehmen darf, werden in § 71 nicht erwähnt. Der Gesetzentwurf (Artikelgesetz) enthält auch keine Änderungen des Sächsischen Versammlungsgesetzes, sodass davon ausgegangen werden darf, dass offene Datenerhebungen bei Versammlungen künftig nicht mittels Drohnen erfolgen dürfen.

XIV. Benachrichtigungspflichten - § 74

In Abs. 1 sollte, wie bereits oben zu § 62a erwähnt, dringend eine Pflicht zur Benachrichtigung der von einer Maßnahme nach § 62a betroffenen Person jedenfalls für die Fälle aufgenommen werden, in denen polizeifremde Datenbestände in die automatisierte Datenanalyse einbezogen wurden (vgl. VIII. zu § 62a Abs. 3 Satz 2).

XV. Befugnis zur Datenverarbeitung - § 79

Mit **Abs. 1** soll laut Begründung eine allgemeine Datenverarbeitungsbefugnis aufgenommen, die es der Polizei erlaubt, personenbezogene Daten zur Aufgabenerfüllung zu verarbeiten, soweit dies erforderlich ist. Auch wenn der zweite Halbsatz der Vorschrift ihre Subsidiarität bestimmt, muss darauf hingewiesen werden, dass ein Rückgriff auf die Generalklausel auch für Weiterverarbeitungen oder Übermittlungen ausgeschlossen ist, die von den spezifischen Weiterverarbeitungs- oder Übermittlungsvorschriften nicht erfasst werden. § 71 Abs. 1 kommt für Weiterverarbeitungen und Übermittlungen also bereits dann nicht zur Anwendung, wenn spezielle Weiterverarbeitungs- und Übermittlungsvorschriften nur vorliegen, unabhängig davon, ob sie besondere Voraussetzungen vorsehen.

Abs. 3 stellt klar, dass die sächsische Polizei die Vorschriften des SächsPVDG auch dann zu beachten hat, wenn sie an einem Informationsverbund teilnimmt bzw. beteiligt ist und personenbezogene Daten in Dateisystemen des Informationsverbundes verarbeitet.

Dies darf nicht dazu führen, dass für den Informationsverbund geltende gesetzliche Regelungen unterlaufen werden (Stichwort: Verbundrelevanz nach § 30 Abs. 1 BKAG). Dabei ist zu beachten, dass z.B. das Bereitstellen von Daten zum Abruf durch andere Verbundteilnehmer bzw. das Einräumen von Zugriffsrechten eine Übermittlung darstellt, die den Anforderungen von § 84 Abs. 1 und § 79a Abs. 2 und 3 zu entsprechen hat.

Dass die seit vielen Jahren übliche Verarbeitung (d.h. in erster Linie Speicherung) von personengebundenen Hinweisen (PHW), die zum Schutz der betroffenen Person oder zum Schutz der Bediensteten der Polizei erforderlich sind, oder weiterer Hinweise, die geeignet sind, dem Schutz Dritter oder der Gewinnung von Ermittlungsansätzen zu dienen (EHW), nunmehr in **Abs. 4** ausdrücklich geregelt wird, ist zu begrüßen.

Die Vergabe von EHW und PHW zu bereits vorliegenden Speicherungen einer Person erfolgt durch ein Schlagwort, das das Risiko einer Stigmatisierung der Person birgt. Während Zuordnungen zu polizeilichen Phänomenbereichen insoweit wenig bedenklich sind, sind „Ein-Wort-Zuschreibungen“ bzw. entsprechende Kürzel, die sich auf per se nicht polizeirelevante Eigenschaften oder Verhaltensweisen der betroffenen Person beziehen, problematisch und geeignet, der betroffenen Person Nachteile bei Kontakt mit der Polizei zu bereiten, die ohne die entsprechenden PHW oder EHW nicht zu befürchten wären. Beispielhaft seien hier die PHW „ANST“ (Ansteckungsgefahr), „PSYV“ (Psychische und Verhaltensstörung) und „LAST“ (Land- oder Stadstreicher) genannt (vgl. LT-Drs. 8/1923).

Diese Risiken müssen bei der Entscheidung über die Vergabe eines PHW oder EHW berücksichtigt werden.

XVI. Zweckändernde Weiterverarbeitung - § 79a Abs. 2

Die Vorschrift bestimmt für die zweckändernde Weiterverarbeitung personenbezogener Daten die Anwendung des Grundsatzes der hypothetischen Datenneuerhebung, wobei der letzte Halbsatz laut Begründung klarstellen soll, dass spezifisch geregelte Weiterverarbeitungsbefugnisse, die eine zweckändernde Verarbeitung von personenbezogenen Daten erlauben, die Regelung des Satz 1 verdrängen. Ob der Wortlaut der Vorschrift dieser Intention Rechnung trägt, ist fraglich. Die Regelung könnte auch so verstanden

werden, dass Satz 1 beachtet werden muss „und“ – kumulativ – die Voraussetzungen einer ggf. bestehenden besonderen Regelung vorliegen müssen.

Klarer wäre eine Bestimmung, wonach besondere Rechtsvorschriften zur zweckändernden Weiterverarbeitung personenbezogener Daten von Satz 1 unberührt bleiben.

XVII. Allgemeine Weiterverarbeitungskonstellationen - § 79b

Abs. 2 soll der Polizei erlauben, 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.

Die Vorschrift ist extrem unbestimmt und knüpft an schwerlich zu belegende subjektive Elemente an. Die subjektive Absicht, eine Straftat zu planen, die auch noch durch eine andere Person begangen werden soll, ist so weit entfernt von objektivierbaren Anknüpfungspunkten, die für polizeiliche Grundrechtseingriffe – wie hier die Verarbeitung personenbezogener Daten – zwingend notwendig sind, dass sie selbst dann, wenn tatsächliche Anhaltspunkte für eine solche Absicht vorliegen sollten, als Voraussetzung für eine Eingriffsbefugnis völlig ungeeignet ist.

Für Zwecke der Gefährderansprache, die die auch eine Information der betroffenen Person über Aussteigerprogramme umschlüsse – die Begründung erwähnt eine „Täteransprache“ –, böte sich eine Orientierung an den bestehenden Regelungen in § 29 POIG BW oder § 12a NPolG an. Beide Vorschriften knüpfen nicht an schwer festzustellende Absichten hinsichtlich der Unterstützung von Straftaten anderer (dritter) Personen an.

In **Abs. 3** wird eine Weiterverarbeitung u.a. zu „archivarischen Forschungszwecken“ geregelt, wobei unklar ist, was mit archivarischen Forschungszwecken gemeint ist.

Eine Weiterverarbeitung personenbezogener Daten zu archivarischen Zwecken richtete sich – ausgenommen die Übermittlung bzw. Überführung von Daten in Unterlagen im archivrechtlichen Sinne an das Archiv, die auf Abs. 3 gestützt werden kann – nach den Bestimmungen des Sächsischen Archivgesetzes.

Zwingend zu beachten ist, dass archivierte personenbezogene Daten nicht wieder in die operative Datenverarbeitung der Polizei überführt werden dürfen, damit grundrechtsschützende polizeigesetzliche (Höchst-)Speicherfristen und Löschungsbestimmungen nicht umgangen werden.

Verfassungsrechtlich problematisch ist die in **Abs. 4** vorgesehene Durchbrechung des Zweckbindungsgrundsatzes nach § 79a und insbesondere des Grundsatzes der hypothetischen Datenneuerhebung nach § 79a Abs. 2 hinsichtlich der Daten, die mittels polizeilicher Befugnisse zur Aufgabenerfüllung der Polizei erhoben wurden. Dies betrifft vorliegend Daten aus polizeilichem Handeln, die zur Vorgangsverwaltung oder zur befristeten Dokumentation behördlichen Handelns gespeichert werden (§ 79 Abs. 2).

So verständlich das Ziel einer Durchbrechung der strengen Zweckbindung des § 79 Abs. 2 für die in hier in Abs. 4 genannten Zwecke wäre – es wäre auch verfassungsrechtlich vertretbar –, so wenig nachvollziehbar und nicht zu rechtfertigen ist eine Ausnahme der Geltung von § 79a Abs. 2 für die polizeiliche Weiterverarbeitung von polizeilich erhobenen Daten.

Eine solche Ausnahme verstieße gegen die Vorgaben des Bundesverfassungsgerichts hinsichtlich des Prinzips der hypothetischen Datenenerhebung und wäre verfassungswidrig.

Das Problem wird anhand folgenden Beispiels deutlich: die Polizei erhebt Daten zur Verhütung einer besonders schweren Straftat. Die Datenerhebung mittels einer besonders eingriffsintensiven Maßnahme sowie daraus erlangte Erkenntnisse werden nach Abschluss des Vorgangs zur zeitlich befristeten Dokumentation behördlichen Handelns gespeichert (befristete Aufbewahrung im Vorgangsbearbeitungssystem nach Abschluss des Vorgangs). Obwohl § 79a Abs. 2 die Weiterverarbeitung für andere Zwecke an enge Voraussetzungen knüpft (Berücksichtigung der Datenerhebungsvorschrift, Verhütung mindestens vergleichbar schwerwiegender Straftat und konkreter Ermittlungsansatz), die im Übrigen auch dann gelten, wenn die Daten vorsorgend gespeichert werden (vgl. § 80 Abs. 4, § 80b Abs. 2), sollen in Durchbrechung dieser verfassungsrechtlich gebotenen Systematik die Daten im Beispiel nun auch zur Verhütung einer Straftat von nur erheblicher Bedeutung verwendet werden dürfen. Wenn Daten aus dem Vorgang, die identisch mit den befristet zur Dokumentation behördlichen Handelns gespeicherten wären, gleichzeitig nach § 80 Abs. 1 oder § 80b Abs. 1 vorsorgend gespeichert würden, dürften letztere wegen der Anordnung der Anwendung von § 79a Abs. 2 (§ 80 Abs. 4 oder § 80b Abs. 2) hingegen nicht zur Verhütung einer Straftat von nur erheblicher Bedeutung weiterverarbeitet werden.

Diese Konsequenz von Abs. 4 kann verfassungsrechtlich nicht gerechtfertigt werden.

Anders liegt der Fall bei der Weiterverarbeitung von Daten aus der Protokollierung nach § 32 Abs. 1 SächsDSUG, die originär nicht zur polizeilichen Aufgabenerfüllung erhoben und verarbeitet, sondern aufgrund einer allgemeinen datenschutzrechtlichen Verpflichtung der verantwortlichen Stelle gespeichert wurden. § 79a Abs. 2 ist insoweit ohnehin nicht einschlägig.

Abs. 4 ist verfassungswidrig, soweit die Regelung für die Weiterverarbeitung von Daten, die die Polizei zur Vorgangsverwaltung oder zur befristeten Dokumentation behördlichen Handelns speichert, eine Ausnahme von § 79a Abs. 2 bestimmt.

Hingenommen werden könnte hingegen eine Durchbrechung der in § 79 Abs. 2 bestimmten Zweckbindung, zwingend erforderlich wäre dann aber, dass die Weiterverarbeitung zu anderen Zwecken als der Vorgangsverwaltung oder der zeitlich befristeten Dokumentation behördlichen Handelns nach Maßgabe von § 79a erfolgte.

XVIII. Training und Test von lernenden KI-Systemen - § 79c

Die Neuregelung ermöglicht die zweckändernde Weiterverarbeitung nahezu sämtlicher rechtmäßig gespeicherter personenbezogener Daten nach einem gestuften Verfahren, das vorrangig Anonymisierung, hilfsweise Pseudonymisierung und ausnahmsweise auch die Verarbeitung von nicht pseudonymisierten personenbezogenen Daten vorsieht.

Zu begrüßen ist das in der Begründung anklingende Bestreben, „durch Training mit polizeilichen Daten nachvollziehbare Datenverarbeitungsschritte in der jeweiligen (eigen-

oder fremdentwickelten) Software unveränderlich zu programmieren und damit die jeweilige spezifische Datenverarbeitung (...) in besonderen Gefahrensituationen durch austrainierte und ausgelernete Systeme zu ermöglichen“.

Der Ausschluss der Anwendung von selbstlernenden KI-Systemen und die Beschränkung auf den Einsatz von austrainierten, deterministischen KI-Modellen in der Ausübung spezifischer Gefahrenabwehrbefugnisse sollte deutlich bereits im Gesetz verankert werden (vgl. VIII. zu § 62a).

Zunächst ist darauf hinzuweisen dass personenbezogene Daten ihren Personenbezug nicht verlieren, wenn sie in selbstlernenden Systemen bzw. lernenden KI-Modellen verarbeitet werden. Der Europäische Datenschutzausschuss (EDSA) hat in seiner Stellungnahme 28/2024 vom 18. Dezember 2024 festgestellt, dass KI-Modelle personenbezogene Daten enthalten können, wenn sie mit personenbezogenen Daten trainiert wurden (https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202428_ai-models_de.pdf). Auch wenn eingegebene personenbezogene Daten in der riesigen Datenmenge z. B. eines sog. Large Language Models LLM „aufgegangen“ sind, ist es nicht völlig unmöglich, die enthaltenen Informationen zumindest in Teilen wieder zu erkennbar zu machen und der betroffenen Person zuzuordnen. Diese sog. Memorisierung personenbezogener Daten birgt erhebliche Risiken.

Personenbezogene Daten, die durch Eingabe in Training oder Test in selbstlernende KI-Systeme eingeflossen sind, werden gewissermaßen Bestandteil des KI-Systems. Bezüglich dieser Daten werden grundrechtsschützende Verpflichtungen der Polizei, denen konkrete Betroffenenrechte korrespondieren (z.B. Auskunft, Löschung, Einschränkung der Verarbeitung), auf Dauer – jedenfalls so lange, wie das trainierte oder getestete KI-System existiert – ausgehebelt bzw. vereitelt.

Es ist vollkommen unklar, wie zum Training oder Test genutzte Daten aus einem KI Modell entfernt werden sollen. Eine entsprechende gesetzliche Anordnung ist nicht umsetzbar, unmöglich zu erfüllen und entfaltet daher keine eingriffsmindernde Wirkung.

Vor diesem Hintergrund ist die Eingriffstiefe bei der Verwendung personenbezogener polizeilicher Daten für das Training und den Test von lernenden KI-Systemen als erheblich zu bewerten. In krassem Widerspruch dazu steht die wenig bis kaum konturierte Befugnisnorm des § 79c.

Abs. 1 formuliert eine pauschale Ermächtigung ohne ausreichende Begrenzungen und ohne auch nur ansatzweise einen Bezug zur polizeilichen Aufgabenerfüllung herzustellen. Weder wird die Befugnis zur Weiterverarbeitung zum KI-Training auf jeweils rechtmäßig gespeicherte personenbezogene Daten beschränkt noch wird eine Eingriffsschwelle für die zweckändernde Weiterverarbeitung bestimmt.

Die oben genannten Risiken und die faktische Beschneidung bzw. der Entzug von Rechten der Personen, deren Daten für Training und Test von selbstlernenden KI-Systemen verwendet werden, wiegen noch einmal deutlich schwerer, wenn die Daten Dritten zur Verfügung gestellt werden – grundsätzlich ermöglichte die Vorschriften Übermittlungen personenbezogener Daten für Trainings- und Testzwecke auch an private Unternehmen in Drittstaaten.

Die Vorschrift trifft keine Unterscheidung hinsichtlich der betroffenen Personenkategorien und erfasst – anders als z.B. die automatisierte Datenanalyse nach § 62a – Anlasspersonen ebenso wie Unbeteiligte.

Gänzlich unberücksichtigt bleiben die Bestimmungen der europäischen KI-Verordnung, die unmittelbar auch im Freistaat Sachsen gilt. Beispielhaft seien hier die Vorschriften zu KI-Reallaboren in Art. 59 KI-VO und das Erfordernis der Einwilligung für Tests unter Realbedingungen außerhalb von Reallaboren genannt (Art. 60, 61 KI-VO).

Bezüglich des letztgenannten Punktes ist bemerkenswert, dass eine Einwilligung betroffener Personen zwar Voraussetzung für eine zeitlich eng begrenzte vorsorgende polizeiliche Speicherung von Daten Unbeteiligter nach § 80a Abs. 1 Satz 2 sein soll, die Verwendung dieser Daten für Training und Test von selbstlernenden KI-Systemen (u.U. durch Dritte in Drittländern) aber voraussetzungslos und ohne Kenntnis der Betroffenen zulässig sein soll.

Das abgestufte Konzept in **Abs. 2**, das die Verwendung von personenbezogenen Daten erst erlaubt, wenn eine vorrangige Anonymisierung oder Pseudonymisierung den Zweck vereitelte oder nur mit unverhältnismäßigem Aufwand möglich wäre, ist als eingriffsmindernde Vorkehrung unrealistisch.

Die Begründung geht davon aus, dass „vorrangig anonymisierte, d.h. nicht personenbezogene, Daten zu verwenden“ seien. In der Praxis ist jedoch eine wirksame Anonymisierung komplexer Datensätze, insbesondere bei biometrischen oder Verhaltensdaten, regelmäßig sehr aufwendig bis unmöglich. Gesichtsbilder z.B. aus Aufzeichnungen der Videoüberwachung öffentlichen Raums können schlechterdings nicht anonymisiert werden, auch eine Pseudonymisierung wird regelmäßig scheitern (vgl. EuGH, Urteil vom 4. September 2025 – C-413/23 P).

Die Vorschrift läuft daher auf eine systematische Verwendung von Klardaten hinaus.

Dass besondere Kategorien personenbezogener Daten gemäß **Abs. 2 Satz 4** nur unter Gewährleistung von Garantien im Sinne des § 4 Absatz 2 SächsDSUG verwendet werden dürfen, ist nur auf den ersten Blick eine Schutzvorkehrung, die praktisch ins Leere läuft. § 4 Abs. 2 SächsDSUG ist ganz offenkundig auf die „klassische“ Verarbeitung der Daten in polizeilichen Vorgangsbearbeitungs- oder Informationssystemen ausgerichtet. Die Mehrzahl der in § 4 Abs. 2 Satz 2 SächsDSUG beispielhaft aufgezählten Garantien ist beim Training oder Test von selbstlernenden IT-Systemen schlicht nicht möglich.

Die Übermittlungsmöglichkeiten an (private) Dritte nach **Abs. 3** sind nicht nur verfassungsrechtlich bedenklich, sondern widersprechen, da Übermittlungen in Drittländern nicht ausgeschlossen werden, auch dem Streben nach (europäischer) digitaler Souveränität. Sie laufen zudem einem zentralen Anliegen der KI-VO zuwider, die mit der Verpflichtung der Mitgliedstaaten zur Bereitstellung von KI-Reallaboren (Art. 59 KI-VO) folgendes Ziel verknüpft: „Innovationen im Bereich KI zu fördern, indem eine kontrollierte Versuchs- und Testumgebung für die Entwicklungsphase und die dem Inverkehrbringen vorgelagerte Phase geschaffen wird, um sicherzustellen, dass die innovativen KI-Systeme mit dieser Verordnung und anderem einschlägigen Unionsrecht und dem nationalen Recht in Einklang stehen“ (Erwägungsgrund 139 KI-VO).

Die in **Abs. 4** formulierten Anforderungen an die Zuverlässigkeit der Datenempfänger kann sich nur auf den ersten Schritt, also die Übermittlung der polizeilichen Daten beziehen. Gelangen die Daten dann in das selbstlernende KI-System, stehen sie – in mehr oder weniger erkennbarer Form – sämtlichen (künftigen) Nutzern des KI-Systems zur

Verfügung (s.o.). Ein substantiierter Schutz für die Betroffenen ergibt sich aus der Vorschrift nicht.

Die Lösungsverpflichtung für Auftrags- und Drittverarbeiter in **Abs. 5 Satz 2** läuft ins Leere. Sie kann sich nur auf die Daten in dem Format beziehen, das die Polizei für Training und Tests übermittelt hat. Eine Löschung der Daten im bzw. aus dem selbstlernenden KI-System ist schlechterdings unmöglich, was den Eingriff in das Recht der Betroffenen vertieft und allgemeine datenschutzrechtliche Schutzbestimmungen aushebelt (s.o.).

Die weitgehende Entgrenzung der Nutzung personenbezogener polizeilicher Daten und die nahezu vollständige Lösung von verfassungsrechtlichen Prinzipien wie der Ausrichtung von Eingriffsnormen an Belangen des Gemeinwohls, der Bestimmtheit von Vorschriften oder der Zweckbindung bzw. Zweckvereinbarkeit zeigen sich in der Möglichkeit, Auftragsverarbeitern und Dritten die Nutzung der mit polizeilichen Daten mit Personenbezug trainierten Modelle für eigene Zwecke einzuräumen, die **Abs. 5 Satz 3** eröffnet. Die Polizei stellte privaten Stellen mit den von ihr übermittelten personenbezogenen und zumeist hoheitlich erhobenen Daten nicht nur den „Rohstoff“ für die Entwicklung und den Betrieb von leistungsfähigen KI-Systemen zur Verfügung, sondern könnte den betreffenden Unternehmen damit auch erlauben, von der fortgesetzten Verarbeitung polizeilicher personenbezogener Daten außerhalb eines polizeilichen Kontextes wirtschaftlich zu profitieren. Angesichts dessen, dass die personenbezogenen Daten, die der Polizei vorliegen und die sie nach Abs. 1 auch an Dritte übermitteln darf, nahezu ausnahmslos aus grundrechtsbeeinträchtigenden Maßnahmen mit teils erheblichem Eingriffsgewicht stammen, bestehen gegen diese „Freigabe“ unter Aufgabe sämtlicher Einflussmöglichkeiten der Polizei **schwerste verfassungsrechtliche Bedenken**.

Die in Abs. 5 Satz 3 bestimmte Voraussetzung, dass aus den trainierten Modellen keine Trainingsdaten abgeleitet werden können, ist unrealistisch und technisch nicht umsetzbar (s.o.). Sie entfaltet daher keine eingriffsmindernde Wirkung.

Abs. 5 Satz 3 wäre daher ersatzlos zu streichen.

Sehr zweifelhaft ist, ob die in **Abs. 6** vorgesehene Verpflichtung zum Erlass von näheren Regeln in einer Verwaltungsvorschrift mit der Wesentlichkeitstheorie vereinbar ist. Wesentliche Entscheidungen muss der Gesetzgeber selbst treffen. Im Entwurf aber werden in § 79c Abs. 1 bis 5, wie erläutert, keine wesentlichen Entscheidungen getroffen. Vermeintliche Schutzbestimmungen erweisen sich als ungeeignet und nicht umsetzbar.

§ 79c weist erhebliche verfassungsrechtliche Defizite auf und sollte grundlegend überarbeitet werden.

Insbesondere sollten die Möglichkeit der Übermittlung an Dritte gestrichen, eine Übermittlung in Drittländer ausdrücklich untersagt und eine Nutzung der mit polizeilichen personenbezogenen Daten trainierten KI-Systeme für eigene Zwecke nicht-öffentlicher Stellen für unzulässig erklärt werden.

XIX. Vorsorgende Speicherung von nicht verantwortlichen Personen - § 80a

§ 80a Abs. 1 Satz 2 setzt für die vorsorgende Speicherung der Personen nach Satz 1 Nummer 1 bis 3 eine Einwilligung dieser Personen voraus, die dann entbehrlich sein soll,

wenn das Bekanntwerden der Speicherungsabsicht den mit der Speicherung verfolgten Zweck gefährden würde.

Unklar ist, an welche Fallgestaltungen in der Praxis hier gedacht ist. Die genannten Personen sind ausnahmslos keine Anlasspersonen, die selbst für eine Gefährdung verantwortlich sind oder – wie der Personenkreis in Nummer 4 – als Kontakt- und Begleitperson (§ 4 Nummer 9) einem besonderen, gefahrgeneigten Näheverhältnis zu einer Anlassperson (§ 80 Abs. 1 Nummer 1 bis 3) stehen.

Die Ausnahme von der Erforderlichkeit einer Einwilligung greift daher unverhältnismäßig in das Recht auf informationelle Selbstbestimmung der Personen nach Nummer 1 bis 3 ein; **der letzte Halbsatz in § 80a Abs. 1 Satz 2 sollte gestrichen werden.**

Fraglich ist, ob bezüglich der Weiterverarbeitung von Daten zu Personen nach Abs. 1 Nummer 1 bis 3 die Anwendung des Prinzips der hypothetischen Datenneuerhebung nach § 79a Abs. 2 sachgerecht und geboten ist. Der Grundsatz wurde im Hinblick auf die Weiterverarbeitung von Daten entwickelt, die mittels Eingriffsbefugnissen über Personen erhoben wurden, die Rechtsgüter gefährdet haben, vor der Begehung von Straftaten standen oder (mutmaßlich) Straftaten begangen haben – auf Zeugen, Opfer/Geschädigte oder Hinweisgeberinnen trifft dies nicht zu – und soll die Verhältnismäßigkeit der zweckändernden Weiterverarbeitung sicherstellen.

Unklar ist insoweit auch das Verhältnis zwischen der konkreten Zweckbestimmung der Speicherung in Abs. 1 – „Verhütung oder zur Vorsorge für die Verfolgung einer Straftat von erheblicher Bedeutung“ –, die konkreter ist als z.B. die Zweckbestimmung in § 80 Abs. 1, und der Anordnung der Geltung von § 79a Abs. 2 für die Weiterverarbeitung in Abs. 3. § 79a Abs. 2 verhinderte die Verwendung von Daten potentieller Geschädigter oder Opfer von Straftaten, deren Daten ursprünglich im Zusammenhang mit der Verhütung (oder Begehung) einer schweren oder besonders schweren Straftat erhoben wurden, für Zwecke der Verhütung einer Straftat von (nur) erheblicher Bedeutung.

Speicherzweck und Weiterverarbeitungsvoraussetzungen stehen nicht in Einklang.

XX. Speicherfristen - § 80d

Abs. 1 erlaubt eine Speicherung personenbezogener Daten, solange wie dies für die Erfüllung der konkreten Aufgabe und des Zwecks, zu dem sie erhoben worden sind, erforderlich ist, und bestimmt konkrete Höchstfristen für Aussonderungsprüfungen.

Spezielle Regelungen für die vorsorgende Speicherung von Daten (§§ 80, 80a, 80b, 80c) folgen in den Absätzen 2 bis 5, womit Abs. 1 für die Dauer der Speicherung personenbezogener Daten in allen anderen Fällen maßgeblich ist. Dazu zählen die Vorgangsbearbeitung, aber auch die Vorgangsverwaltung und die befristete Dokumentation behördlichen Handelns (§ 79 Abs. 2). Angesichts dieses Spektrums ist fraglich, ob die speicherzweckunabhängige Bestimmung von Höchstfristen und die gleichzeitige Festlegung des Fristbeginns sachgerecht und verhältnismäßig ist. Für langwierige Vorgangsbearbeitungen können die Fristen im Einzelfall nicht ausreichend sein, für die Speicherung von Daten zur befristeten Dokumentation behördlichen Handelns erscheinen sie – insbesondere hinsichtlich geringfügiger Vorkommnisse mit einem zügigen Abschluss des Verfahrens – zu lang und damit datenschutzrechtlich bedenklich (bislang gilt für die Speicherung im Vorgangsbearbeitungssystem eine zweijährige Aufbewahrungsfrist, die mit Abschluss des Vorgangs beginnt).

Mit der Festlegung kürzerer Aussonderungsprüffristen, die mit Abschluss des Vorgangs beginnen, könnten polizeifachliche und verfassungsrechtliche Belange gleichermaßen angemessene Berücksichtigung finden.

Die Bestimmung möglichst kurzer Speicherfristen ist auch im Hinblick auf die weitreichenden und eingriffsintensiven Verarbeitungsbefugnisse im Rahmen der automatisierten Datenanalyse (§ 62a) und zum Training und Test von lernenden KI-Systemen (§ 79c) zwingend notwendig.

Nicht geregelt ist in Abs. 1 der Fall, dass die Aussonderungsprüfung zum Ergebnis hat, dass die Daten weiterhin zur Aufgabenerfüllung erforderlich sind (§ 80d Abs. 4 trifft insoweit Bestimmungen nur für Fälle der vorsorgenden Speicherung). Zumindest die Pflicht zur dokumentierten Begründung einer Entscheidung für die Speicherung über die Aussonderungsprüffrist hinaus sollte aufgenommen werden.

Unklar ist, aus welchen Gründen **§ 80d Abs. 3 Satz 1 Nr. 1** spezielle Aussonderungsprüffristen für Verurteilte vorsieht (Personen nach § 80 Abs. 1 Satz 1 Nr. 1). Die Verurteilung wegen einer Straftat allein lässt keine Rückschlüsse auf die Gefährlichkeit der Person bzw. die Relevanz ihrer Daten für die polizeiliche Aufgabenerfüllung zu. Das aber sind die entscheidenden Kriterien für eine verfassungsgemäße vorsorgende Speicherung. Maßgeblich ist nicht das Vorliegen eines Urteils zu einer in der Vergangenheit liegenden Handlung, sondern die aktuelle polizeiliche Bewertung der gefahrenabwehrrechtlichen Relevanz der Person. Die polizeiliche Speicherung dient anderen Zwecken als zum Beispiel das Bundeszentralregister; die Polizei ist weder Registerbehörde noch Gerichtsarchiv.

Der Gesetzentwurf entkoppelt in § 80 Abs. 1 Satz 2 in ausdrücklich zu begrüßender Weise die Erforderlichkeit einer Negativprognose für eine vorsorgende Speicherung von den Umständen des Ausgangs des strafprozessualen Verfahrens. Dieser Ansatz sollte konsequent verfolgt werden und damit auch in § 80d Abs. 3 angewandt werden:

Die Fristen nach § 80d Abs. 3 Satz 1 Nr. 2 Buchst. a und b sollten auch in Bezug auf Speicherungen zu verurteilten Personen gelten.

Soweit § 80d Abs. 3 Satz 1 Nr. 1 (Verurteilte) und Nr. 2 (Beschuldigte) Speicherfristen für Kinder vorsehen, muss darauf hingewiesen werden, dass Kinder – also Personen vor Vollendung des 14. Lebensjahres – aufgrund ihrer Strafunmündigkeit (§ 19 StGB) unter keinen Umständen wegen einer Straftat verurteilt werden können bzw. dürfen. Die fehlende Strafmündigkeit führt auch dazu, dass Kinder keine Beschuldigten im Sinne der Strafprozessordnung und in der Verwendung nach Nr. 2 sein können.

Die Personengruppe der Kinder ist den Vorschriften § 80d Abs. 3 Satz 1 Nr. 1 und Nr. 2 zu streichen.

XXI. Datenübermittlung im innerstaatlichen Bereich - § 84

Angesichts dessen, dass Übermittlungen der Polizei zur Erfüllung eigener Aufgaben in erster Linie in der konkreten Vorgangsbearbeitung erfolgen dürften, könnte ein Ausschluss der Anwendbarkeit von § 79a Abs. 1 (zweckwahrende Nutzung) zu verfassungsrechtlich nicht erforderlichen Einschränkungen der polizeilichen Vorgangsbearbeitung führen.

Die in den Abs. 1, 2 und 3 formulierte Anordnung der Geltung von § 79a Abs. 2 und 3 sollte daher – allerdings ausschließlich für die Variante der Übermittlung zur eigenen Aufgabenerfüllung – um die Geltung von § 79a Abs. 1 erweitert werden.

Gegen die Befugnis, personenbezogene Daten ohne Einwilligung der betroffenen Person nach **Abs. 3 Nr. 4** an eine private Beratungsstelle zu übermitteln, sofern die Polizei Bedarf für eine Beratung zum Schutz vor häuslicher Gewalt feststellt, bestehen **schwere datenschutzrechtliche Bedenken**. Eine solche Übermittlung greift unverhältnismäßig in das Recht der betroffenen Person auf informationelle Selbstbestimmung ein. Dabei ist zu betonen, dass das Ziel der Befugnis, nämlich die Unterstützung von Personen in einer schwierigen Situation, nicht zu kritisieren ist. Allerdings ist das Interagieren von Privaten prinzipiell ein privater Vorgang, der von privater Seite aus initiiert werden sollte. Das staatliche „Erzwingen“ eines Kontaktes von nichtstaatlichen Akteuren ist abzulehnen.

Es bestehen strake Zweifel daran, dass ein Vorgehen nach Abs. 3 Nr. 4 für betroffene Personen hilfreicher wäre als sie beispielsweise mündlich, schriftlich, per Flyer über Hilfsangebote zu informieren und ihnen selbst die Entscheidung zu überlassen, ob – und vor allem, wann – sie Kontakt zu einer Beratungsstelle aufnehmen. Von häuslicher Gewalt betroffene Personen, die möglicherweise in einem Abhängigkeitsverhältnis zum Verursacher stehen und in ihrer Alltagsgestaltung unter dessen Kontrolle stehen, können selbst am besten über einen geeigneten Zeitpunkt einer Kontaktaufnahme entscheiden; eine „staatlich verordnete“ Kontaktaufnahme durch die Beratungsstelle „zur Unzeit“, die dem Gewalttäter eventuell zur Kenntnis gelangt, ist zu vermeiden.

Abs. 3 Nr. 4 sollte ersatzlos gestrichen werden.

Dem absolut förderungswürdigen und unterstützungswerten Anliegen, Opfern häuslicher Gewalt zu helfen, muss und kann auf andere Weise Rechnung getragen werden.

XXII. Zuverlässigkeitsüberprüfungen vor gefährdeten Veranstaltungen - § 88

Hinsichtlich der in **Abs. 3** genannten Stellen, die in die Zuverlässigkeitsüberprüfung einbezogen werden können, ist nicht nachvollziehbar, aus welchem Grund nach **Nr. 3** auf den Datenbestand des **Bundesamtes für Migration und Flüchtlinge (BAMF)** zurückgegriffen werden sollte. Es ist schwer vorstellbar, dass im BAMF relevante sicherheitsrelevante Erkenntnisse zu Personen vorliegen, über die die Polizei und/oder Verfassungsschutzbehörden nicht in Kenntnis gesetzt wurden. Die Sicherheitsbehörden erhalten vom BAMF Informationen über Drittstaatsangehörige, die eine Gefahr für die Sicherheit der Bundesrepublik und die freiheitliche demokratische Grundordnung aufzeigen. Das BAMF unterrichtet von sich aus das Bundesamt für Verfassungsschutz (§§ 3 Abs. 1, 18 Abs. 1a BVerfSchG) und das Bundeskriminalamt, § 9 Abs. 4 BKAG

(https://www.bamf.de/SharedDocs/Anlagen/DE/EMN/Studien/wp86-umgang-gefaehrder.pdf?__blob=publicationFile&v=13, S. 27).

Angesichts dieser Umstände sollte Abs. 3 Nr. 3 gestrichen werden. Relevante Erkenntnislücken wären nicht zu befürchten.

Die strenge Zweckbindung in **Abs. 4 Satz 2** sollte mit Blick auf die weiten und eingriffsintensiven Verarbeitungen polizeilicher Daten nach § 62a und § 79c mit einem Verbot der Aufnahme der für Zwecke der Zuverlässigkeitsüberprüfung erhobenen Daten in den „operativen Datenbestand“ der Polizei flankiert werden. Der Maßnahme der Zuverlässigkeitsüberprüfung liegt keine polizeiliche Gefahr zugrunde, sie wird nicht selten durch private Stellen (Veranstalter) initiiert, denen die Letztentscheidung über die Gewährung eines privilegierten Zugangs der betroffenen Person zu der Veranstaltung obliegen. Die Polizei agiert insoweit als Dienstleister und erhebt in dieser Funktion Daten, die sie mangels Relevanz für ihre Aufgabenerfüllung ohne das Ersuchen des Veranstalters nicht erhoben hätte.

Vor diesem Hintergrund ist eine gesonderte Speicherung der erhobenen Daten und eine an der Zweckbindung von Abs. 4 Satz 2 orientierte Begrenzung ihrer Weiterverarbeitung für andere Zwecke zwingend geboten.

Die in **Abs. 6** vorgesehene **Speicherfrist** von sechs Monaten ist nicht zu beanstanden; sie wird aber durch die Festlegung des Fristbeginns in **Abs. 6 Satz 2** je nach Einzelfall unverhältnismäßig lang. Theoretisch kann die Speicherdauer bis zu 18 Monate betragen. Eine verfassungsrechtlich tragfähige Rechtfertigung für eine solche Aufbewahrungsfrist ist nicht ersichtlich.

Abs. 6 Satz 2 wäre zu streichen, sachgerecht wäre ein Fristbeginn bei Abschluss der polizeilichen Prüfung der Zuverlässigkeit und Mitteilung des Ergebnisses an Veranstalter und betroffene Person (Abs. 4).

XXIII. § 30 SächsPBG

Mit der Änderung von § 30 Abs. 1 soll das Urteil des Sächsischen Verfassungsgerichtshofes vom 25. Januar 2024 umgesetzt werden, wonach die Vorschrift des bisherigen § 30 Abs. 1 Nummer 2 SächsPBG nicht den Anforderungen an die Bestimmtheit und Normenklarheit genüge (Verfassungsgerichtshof des Freistaates Sachsen, Urteil vom 25. Januar 2024 – Vf. 91-II-19 –, Rn. 388, juris).

Während gegen die Bestimmung der Eingriffsschwelle in der Regelung des künftigen § 30 Abs. 1 Nummer 2 keine Bedenken bestehen, ist eine Verbesserung der Bestimmtheit der Norm hinsichtlich der Örtlichkeiten in **§ 30 Abs. 1 Nr. 1** leider nicht zu konstatieren.

Zwar werden nun neben den „öffentlichen Einrichtungen“ weitere Örtlichkeiten aufgezählt, wobei es zu Überschneidungen bzw. Unklarheiten kommt (Dienstgebäude werden gesondert genannt, laut Begründung aber sollen z.B. Rathäuser „öffentliche Einrichtungen“ sein). Mit der Aufnahme des unbestimmten und in der Begründung nicht erläuterten Begriffs der „sonstigen baulichen Anlagen öffentlicher Stellen“ aber resultiert aus der Betrachtung des örtlichen Anwendungsbereichs der Vorschrift, der zudem die unmittelbare

Nähe der Örtlichkeiten umfasst, eine Unklarheit und Unbestimmtheit, die im Vergleich zur bisherigen Rechtslage nicht reduziert wurden.

Zwar ergibt sich aus der klareren Eingriffsschwelle – laut Begründung wird das Vorliegen einer entsprechenden Tatsachenbasis vorausgesetzt, die geeignet ist, die Prognose künftiger Gefahren für die Rechtsgüter von Leib oder Leben oder bedeutende Sach- oder Vermögenswerte zu begründen – eine Begrenzung der Anwendungsmöglichkeit der Befugnisnorm, gleichwohl sollte aus Gründen der Normenklarheit und Rechtssicherheit die Angabe der Örtlichkeiten in Nr. 1 präzisiert werden.

Aufgrund der leider noch immer mangelnden örtlichen Bestimmtheit der Norm des § 30 Abs. 1 Nr. 1 sollte zumindest das Verbot einer flächendeckenden Videoüberwachung im Gemeindegebiet gesetzlich verankert werden.

Eine Präzisierung der Bestimmung hinsichtlich der Örtlichkeiten wäre auch im Hinblick auf die augenscheinlichen Überschneidungen der Anwendungsbereiche von § 30 Abs. 1 Nr. 1 und § 13 Abs. 1 SächsDSDG dringend geboten. Soweit die Begründung als Beispiele einer „öffentlichen Einrichtung“ im Sinne von § 30 Abs. 1 Nr. 1 „Rathäuser, Museen, Sportplätze, öffentliche Schwimmbäder, Kanalisation, Wertstoffhöfe“ erwähnt, ist darauf hinzuweisen, dass die Videoüberwachung derartiger Einrichtungen durch die Kommunen bislang auf § 13 SächsDSDG – entweder in Wahrnehmung des Hausrechts oder zur Aufgabenerfüllung – gestützt werden konnte (https://www.datenschutz.sachsen.de/download/Orientierungshilfe_fuer_die_Videoeubewachung_durch_saechsische_Kommunen.pdf, S. 11).

Die Aufzählung der Beispiele (hier insbesondere Museen, Sportplätze, öffentliche Schwimmbäder, Kanalisation, Wertstoffhöfe) einerseits und der Hinweis in der Begründung, dass die Videoüberwachung an diesen Orten „dem Vollzug der gemeindlichen Aufgabe der Gefahrenabwehr als Ortspolizeibehörde dient“, andererseits sind schwer in Einklang zu bringen, konnten solche Einrichtungen bislang doch zur Aufgabenerfüllung der besonderen kommunalen Gefahrenabwehrbehörden oder Ämter „kommunalaufgabenspezifisch“ nach § 13 Abs. 1 SächsDSDG videoüberwacht werden.

Die Bestimmung in § 30 Abs. 1 Nr. 1 legt in der Zusammenschau mit ihrer Begründung nahe, dass künftig – auch im Hinblick auf die Subsidiarität des SächsDSDG nach § 2 Abs. 5 SächsDSDG – die Videoüberwachung kommunaler öffentlicher Einrichtungen nicht mehr nach § 13 Abs. 1 SächsDSDG zur Aufgabenerfüllung der Kommune erfolgen darf, sondern ausschließlich nach und unter den Voraussetzungen von § 30 Abs. 1 Nr. 1.

In datenschutzrechtlicher Hinsicht wäre das zu begrüßen, da die Voraussetzungen von § 30 Abs. 1 Nr. 1 nicht nur höher, sondern auch bestimmter sind als die „Erforderlichkeit“ zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, die nach § 13 Abs. 1 SächsDSDG vorausgesetzt wird.

Die neue Befugnis der Videoüberwachung **in** öffentlichen Einrichtungen und Dienstgebäuden kollidiert mit der Befugnis öffentlicher Stellen zur Videoüberwachung in Wahrnehmung des Hausrechts nach § 13 Abs. 1 SächsDSDG.

Auch in diesem Zusammenhang stellt sich durch die Neuregelung die Frage, ob eine Videoüberwachung zur Wahrnehmung des Hausrechts nach § 13 Abs. 1 SächsDSDG künftig durch § 30 Abs. 1 Nr. 1 verdrängt wird.

Vor diesem Hintergrund sollte die Vorschrift überarbeitet und das Verhältnis zu § 13 Abs. 1 SächsDSDG geklärt werden.

Für die Berücksichtigung meiner Hinweise im weiteren Verfahren wäre ich Ihnen dankbar.

Mit freundlichen Grüßen
Im Auftrag

gez. Mauersberger
Referatsleiter