**SCHLESWIG-HOLSTEINISCHER LANDTAG** **Drucksache 20/4284**
**20. Wahlperiode** 24. März 2026

## Gesetzentwurf

der Landesregierung – Ministerin für Inneres, Kommunales, Wohnen und Sport

# Gesetz zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit

## A. Problem

Die Notwendigkeit zur beständigen Fortentwicklung polizeirechtlicher Maßnahmen ergibt sich im Besonderen durch technische Entwicklungen, die für eine moderne und effiziente Gefahrenabwehr unverzichtbar geworden sind. In einem digitalisierten Umfeld hängt die Wirksamkeit polizeilicher Arbeit in erheblichem Maße davon ab, dass vorhandene Informationen in der erforderlichen Zeit vollständig und zutreffend verfügbar sind. Die notwendige Weiterentwicklung des Polizeirechts betrifft im Allgemeinen aber auch die tradierten und etablierten Rechtsgrundlagen. Eingeführte Standardermächtigungen sind zu überprüfen und dort, wo sich Wirksamkeitsdefizite oder Schutzlücken zeigen, ist das geltende Recht effizienter zu gestalten.

Der Anstoß zu diesem Gesetzentwurf waren gravierende Messerangriffe in der Öffentlichkeit. Vor dem Hintergrund des Anschlags in Solingen am 23. August 2024 hat die Landesregierung – gemeinsam mit der Regierung des Landes Nordrhein-Westfalen – am 17. September 2024 ein Maßnahmenpaket in den Bereichen Sicherheit, Migration und Prävention beschlossen. Die Initiativen im Bereich Sicherheit dieses Maßnahmenpakets setzt der vorliegende Gesetzentwurf um. Der Messerangriff in der Kieler Innenstadt am 25. Januar 2025 hat Handlungsbedarf innerhalb der bestehenden Befugnisse offengelegt, die im Einzelfall gestatten, einer Person vorübergehend die Freiheit zu entziehen, wenn dies zur Abwehr erheblicher Gefahren für Rechtsgüter von Bürgerinnen und Bürgern unerlässlich ist. Zudem wurde deutlich, dass die Möglichkeit, den Aufenthaltsort einer Person, von der erhebliche Gefahren für andere Menschen ausgehen, mittels einer sogenannten Fußfessel zu überwachen, in Schleswig-Holstein beschränkt ist und bestimmte Konstellationen nicht abdeckt.

Dem Phänomen der „Messerangriffe“ wirksam entgegenzutreten, ist nach wie vor eine vordringliche Aufgabe der Gefahrenabwehr. Die Polizeiliche Kriminalstatistik (PKS) wies im Berichtsjahr 2024 erstmals „Messerangriffe“ aus. Ihre Zahl bezifferte die Statistik für dieses Berichtsjahr bundesweit auf 29.014 Straftaten. Davon entfielen 54,3 Prozent auf Gewaltkriminalität, 43,3 Prozent auf Bedrohung und 2,4 Prozent auf sonstige Straftaten, wie beispielsweise Widerstand gegen und tätlicher Angriff auf Vollstreckungsbeamtinnen und -beamte und gleichstehende Personen sowie Nötigung. Eine vergleichende Betrachtung der PKS-Daten weist zudem auf eine kontinuierlich steigende Anzahl von Messerangriffen im Bereich der gefährlichen und schweren Körperverletzungen hin: Im Jahr 2022 wurden bundesweit 8.160, im Folgejahr 8.951 und im Jahr 2024 schließlich 9.917 Straftaten in diesem Deliktsfeld registriert. Neben den Körperverletzungen sind zur Beurteilung der Messerkriminalität auch die Tötungsdelikte in den Blick zu nehmen. Von den in der PKS im Berichtsjahr 2024 verzeichneten insgesamt 2.303 Fällen des Mordes, des Totschlags und der Tötung auf Verlangen sind 922 dieser Straftaten (40,0 Prozent) als Messerangriffe eingestuft. Messerangriffe in der Öffentlichkeit – neben den bereits erwähnten Taten müssen mindestens auch die Taten in Aschaffenburg im Januar 2025, in Mannheim im Mai 2024 und Brokstedt im Januar 2023 genannt werden – stehen besonders im gesellschaftlichen Fokus.

Die mit diesem Gesetzentwurf im Gefahrenabwehrrecht des Landes umzusetzenden Änderungen sind aber nicht nur als Maßnahmen gegen Messerangriffe zu verstehen, son-

dern stellen notwendige Weiterentwicklungen verschiedener polizeirechtlicher Instrumente zur Verbesserung des Schutzes der öffentlichen Sicherheit dar. Ziel des Maßnahmenpakets vom 17. September 2024 ist die Handlungsfähigkeit der Landespolizei insgesamt durch den Einsatz von technischen Weiterentwicklungen – Nutzung von Künstlicher Intelligenz, Gesichtserkennungssoftware und automatisierter Datenanalyse – zu sichern und zu stärken. Die Standardbefugnisse zum Polizeigewahrsam und zur elektronischen Aufenthaltsüberwachung sind zu verbessern, um Schutzlücken zu schließen. Gleichermaßen aber gilt es diese Regelungsmaterien insgesamt zu reformieren und zu modernisieren, einschließlich ergänzender Vorschriften und des bereichsspezifischen Verfahrensrechts.

## B. Lösung

Der Gesetzentwurf entwickelt verschiedene Instrumente des Polizeirechts weiter:

- Neue Formen der Nutzung polizeilicher Datenbestände durch Datenabgleich werden im Gefahrenabwehrrecht implementiert, um Gefahren und Störerinnen und Störer durch eine effizientere Datenverarbeitung zielgerichtet und früher zu identifizieren.
- Die Videoüberwachung im öffentlichen Raum wird ausgebaut und durch den Einsatz automatischer Anwendungen zur Mustererkennung effektiver gemacht.
- Schutzlücken im System der Regelungen, die eine Ingewahrsamnahme oder elektronische Überwachung von Personen dann vorsehen, wenn dies im Einzelfall zur Abwehr von erheblichen Gefahren unerlässlich ist, werden geschlossen.

Im Einzelnen:

Das Landesverwaltungsgesetz (LVwG) kennt zwei Formen des Datenabgleichs. Gemäß § 195 LVwG kann die Polizei bei einem einfachen Datenabgleich maschinell-automatisch per Systemabfrage in Datenbanken abklären, ob und gegebenenfalls welche Daten über eine bestimmte Person bereits gespeichert sind. Eine besondere Form des Datenabgleichs ist die Rasterfahndung gemäß § 195a LVwG. Sie gestattet die Durchsuchung ganzer Datenbestände, die zu diesem Zweck von anderen Stellen angefordert werden. Ziel ist es, anhand bestimmter Suchkriterien Personen zu identifizieren, die für eine Gefahrenlage verantwortlich sind. Zu den bestehenden Formen des Datenabgleichs fügt dieser Gesetzentwurf zwei neue Formen hinzu:

- Die automatisierte **Datenanalyse** ermöglicht im Einzelfall die Weiternutzung großer und komplexer Informationsbestände. Häufig sind Informationen nicht im gleichen Bearbeitungskontext simultan verfügbar, weil sie unstrukturiert vorliegen und in unterschiedlichen Formaten und in disparaten Dateien gespeichert sind. Die automatisierte Datenanalyse überwindet diese Grenze. Mit ihr können unterschiedliche Datenbestände zusammengeführt und Strukturen, Muster und Zusammenhänge sichtbar gemacht werden, die ein Mensch, auch wenn er Zugang zu allen diesen Informationen hätte, so nicht oder kaum hätte erkennen können. Die Polizei erhält damit ein Instrument, um Personen zu identifizieren, die Gewalttaten vorbereiten, ankün-

digen oder deren Radikalisierung eine Tatgeneigtheit hervorgebracht hat. Mit der automatisierten Datenanalyse allein kann die Gewalttat nicht verhindert werden; sie ist jedoch ein Mittel, das gefahrenabwehrende Maßnahmen wirksamer macht, indem es Hintergründe und relevante Informationen aufzeigt, zusammenfügt und strukturiert abbildet.

- Die **biometrische Fernidentifizierung** ermöglicht es, Personen ohne ihre aktive Einbeziehung und in der Regel aus der Ferne durch Abgleich ihrer biometrischen Daten mit gespeicherten biometrischen Referenzdaten zu identifizieren. Die Referenzdaten können aus unterschiedlichen Quellen stammen: Daten, die rechtmäßig in polizeilichen Systemen gespeichert sind, aus dem Internet erlangte öffentlich zugängliche Daten oder in Echtzeit im öffentlichen Raum aufgenommene Bild- oder Tonaufzeichnungen. In einer digitalisierten Welt erschließt die Fernidentifizierung neue Erkenntnisquellen für die Gefahrenabwehr. Mit ihr können Fahndungsmaßnahmen unterstützt werden; sie beschränkt sich aber nicht ausschließlich auf das Aufspüren flüchtiger Personen, sondern kann auch zum Schutz von gefährdeten Personen eingesetzt werden, unter bestimmten Voraussetzungen etwa zum Auffinden vermisster Personen oder von Opfern des Menschenhandels.

Durch eine Videoüberwachung des öffentlichen Raums kann eine positive Wirkung auf die Sicherheitslage an Kriminalitäts- oder Gefahrenschwerpunkten erreicht werden. Rechtsgrundlage für den Einsatz von Videotechnik ist § 184 LVwG. Diese Befugnis baut der Gesetzentwurf aus:

- Die allgemein zugänglichen oder für die Allgemeinheit geöffneten Bereiche, die mittels offener **Bild- und Tonaufnahmen oder -aufzeichnungen** überwacht werden können, werden um gefährliche und gefährdete Orte (§ 181 Absatz 1 Nummer 1 bis 3 LVwG) erweitert. Um der Entwicklung mobiler Überwachungstechnik Rechnung zu tragen, kann künftig eine Videoüberwachung anlassbezogen bei einer konkreten Gefahrenlage kurzfristig eingerichtet werden. Durch den Einsatz technischer Möglichkeiten zur Mustererkennung sollen Schwächen der manuellen Überwachung ausgeglichen werden.

Im Einzelfall kann es unerlässlich sein, die Person, von der eine erhebliche Gefahr ausgeht, zu überwachen und ihr im äußersten Fall aus präventiven Gründen für einen bestimmten Zeitraum die Freiheit zu entziehen. Die Ingewahrsamnahme gemäß §§ 204, 205 LVwG gehört zu den tradierten Instrumenten polizeilichen Handelns. Ein modernes milderes Mittel gegenüber der Freiheitsentziehung stellt in bestimmten Fallkonstellationen die Möglichkeit dar, den Aufenthaltsort der Person mittels einer sogenannten „elektronischen Fußfessel“ zu überwachen. Beide Instrumente gestaltet der Gesetzentwurf neu:

- Die Tatbestände für einen **Präventivgewahrsam** werden überarbeitet. Die Möglichkeit de lege lata, eine Person zur Verhinderung einer unmittelbar bevorstehenden Begehung oder Fortsetzung einer Straftat in Gewahrsam zu nehmen, wird im Gesetzestext um bestimmte Anknüpfungstatsachen (Bekenntnis zur Tat, das Auffinden bestimmter Gegenstände und die Wiederholungsgefahr)

ergänzt, um in der Praxis die Gefahrenprognose zu vereinheitlichen und die Vorhersehbarkeit zu erhöhen. Außerdem wird ein neuer Gewahrsamstatbestand bei konkreten Gefahren für besonders wichtige Rechtsgüter (Leib, Leben, Freiheit der Person und sexuelle Selbstbestimmung) als Auffangtatbestand eingeführt. Die Behandlung der in Gewahrsam genommenen Person und die Verfahrensvorschriften werden reformiert.

- Der Einsatz der **elektronischen Aufenthaltsüberwachung** zum Schutz besonders wichtiger Individualrechtsgüter wird erweitert und dadurch als milderes Mittel gegenüber dem Präventivgewahrsam gestärkt. Aktuell gestattet § 201c LVwG eine solche Maßnahme nur zum Schutz einer bestimmten Person. Der neu gestaltete § 201b LVwG-Entwurf ermöglicht den Einsatz der sogenannten „elektronischen Fußfessel“ auch dann, wenn das Überwachungsziel der Schutz von Personen ist, die nicht individuell, sondern nur anhand bestimmter Kriterien oder Gruppenzugehörigkeiten bestimmbar sind. Die primäre Schutzrichtung der elektronischen Aufenthaltsüberwachung, Femizide und gleichgelagerte Gewalttaten und Stalking zu verhindern, bleibt nach der Neufassung von § 201b LVwG-Entwurf unverändert erhalten.

## C. Alternativen

Keine.

## D. Kosten und Verwaltungsaufwand

Abweichend von den in den nachfolgenden Absätzen aufgeführten bereits vorhandenen Haushaltsmitteln stehen alle zukünftigen weiteren Kosten und Verwaltungsaufwände grundsätzlich unter Haushaltsvorbehalt.

### 1. Kosten

Für das **Maßnahmenpaket Sicherheit, Migration und Prävention** wurden im Haushalt 2025 für den Polizeibereich 1.290 T€ bei Kapitel 0410 und 4.700 T€ bei Einzelplan 14 zur Verfügung gestellt. Für Investitionen überwiegend im IT-Haushalt stehen 3.730 T€ zur Verfügung, für strukturelle Ausgaben sind jährlich 1.595 T€ veranschlagt. Hinzu kommen Personalausgaben für 19 neue Planstellen und Stellen in Höhe von 665 T€. Davon entfallen auf die polizeirechtlichen Instrumente, auf die sich der vorgelegte Gesetzentwurf bezieht, 2.420 T€, davon 1.800 T€ für Investitionen, 370 T€ für Betriebskosten und Personalausgaben für fünf Stellen in Höhe von 250 T€.

Mit der Novellierung der Vorschriften zum **Polizeigewahrsam** ist ein weiterer Anstieg von Fällen zu erwarten, in denen längerfristige Ingewahrsamnahmen angeordnet und in Justizvollzugsanstalten im Wege der Amtshilfe vollzogen werden. Während von 2021 bis 2023 eine nur niedrige einstellige Zahl solcher Fällen zu verzeichnen gewesen ist, ist seit 2024 ein Anstieg festzustellen. Im Jahr 2025 ist in 13 Fällen ein längerfristiger Polizeige-

wahrsam (insgesamt 141 Tage) angeordnet und in den Justizvollzugsanstalten des Landes vollzogen worden. Es ist davon auszugehen, dass diese Tendenz durch den vorgelegten Gesetzentwurf verstärkt werden wird, ohne dass sich diesbezüglich konkrete Zahlen prognostizieren lassen.

Durch die Erweiterung der Befugnis zur **elektronischen Aufenthaltsüberwachung**, die der vorgelegte Gesetzentwurf herbeiführt, ist ebenfalls mit einem Anstieg dieser Maßnahmen zu rechnen. Für die Durchführung der elektronischen Aufenthaltsüberwachung im Bereich der Führungsaufsicht ist auf der Basis eines Staatsvertrages im Bundesland Hessen eine gemeinsame elektronische Überwachungsstelle der Länder (GÜL) errichtet worden. Diese Strukturen können aktuell für die Durchführung der elektronischen Aufenthaltsüberwachung im Bereich der Gefahrenabwehr im Wege der Amtshilfe genutzt werden.

## 2. Verwaltungsaufwand

Die Einführung und der Betrieb der mit dem **Maßnahmenpaket Sicherheit, Migration und Prävention** vorgesehenen technischen Instrumente für moderne Formen des Datenabgleichs, nämlich die automatisierte Datenanalyse und die biometrische Fernidentifizierung, und die Ausweitung der Videoüberwachung im öffentlichen Raum einschließlich der Etablierung von Software zur Bewegungsmustererkennung sind zunächst ein erhöhter Verwaltungsaufwand im Zusammenhang mit dem Aufbau der erforderlichen IT-Infrastruktur, der Gewährleistung der Datensicherheit und des Datenschutzes sowie Schulungs- und Fortbildungsbedarfe zu erwarten. Die Mehraufwände können innerhalb der vorhandenen Ressourcen kompensiert werden. Umgekehrt ist mittelfristig zu berücksichtigen, dass der Einsatz der genannten technischen Instrumente zu einer Effektivierung der Polizeiarbeit und Verringerung der Belastung von Mitarbeiterinnen und Mitarbeitern der Polizei führen wird.

Für die Polizei bedeutete der bereits seit 2024 zu verzeichnende Anstieg von Fällen des **längerfristigen Polizeigewahrsams** einen erhöhten, aber noch zu bewältigenden Verwaltungsaufwand. Die Entwicklung der Belastung durch einen weiteren Anstieg der Fallzahlen bleibt abzuwarten. Bezogen auf den jeweiligen Einzelfall ist kein höherer Verwaltungsaufwand zu erwarten, da keine weiteren oder neuen Verwaltungsschritte im Einzelfall erwachsen. Für den Justizvollzug bedeutet der Anstieg der längerfristigen Ingewahrsamnahmen einen höheren Verwaltungsaufwand, der nicht beziffert werden kann.

Für die Polizei bedeutet die Ausweitung der **elektronischen Aufenthaltsüberwachung** über den Kontext von Partnerschaftsgewalt hinaus einen Mehraufwand, der noch nicht beziffert werden kann. Erforderlich wird im Einzelfall eine polizeiliche Überprüfung der durch technische Meldungen bei der GÜL angezeigten Verstöße. Hierfür werden innerhalb der bestehenden Strukturen Mechanismen zur Entgegennahme und Steuerung der eingehenden Meldungen mit entsprechender technischer und personeller Ausstattung zu entwickeln sein.

### 3. Auswirkungen auf die private Wirtschaft

Es sind keine Auswirkungen auf die private Wirtschaft zu erwarten.

## E. Nachhaltigkeit

Das Vorhaben hat positive Auswirkungen auf „Good Governance und gesellschaftliche Teilhabe“. Das Vorhaben hat keine direkten oder indirekten Auswirkungen auf die Treibhausgasemissionen.

## F. Länderübergreifende Zusammenarbeit

Keine.

## G. Informationen des Landtags nach Artikel 28 der Landesverfassung

Die Präsidentin des Schleswig-Holsteinischen Landtages wird über den Gesetzentwurf nach der ersten Kabinettsbefassung unterrichtet.

## H. Federführung

Federführend ist die Ministerin für Inneres, Kommunales, Wohnen und Sport.

# Gesetz zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit

**Vom**

Der Landtag hat das folgende Gesetz beschlossen:

## Artikel 1
## Änderung des Landesverwaltungsgesetzes

Das Landesverwaltungsgesetz in der Fassung der Bekanntmachung vom 2. Juni 1992 (GVOBl. Schl.-H. S. 243, ber. S. 534), zuletzt geändert durch *[Schriftstelle bitte einsetzen: aktuellste Änderung und Fundstelle]* wird wie folgt geändert:

**1. Die Inhaltsübersicht wird wie folgt geändert:**

**a) Die Angabe zu § 184 erhält folgende Fassung:**

„§ 184 Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an allgemein zugänglichen Orten“

**b) Nach der Angabe zu § 184a werden folgende Angaben eingefügt:**

„§ 184b Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen“

„§ 184c Durchführung der Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen“

**c) Nach der Angabe zu § 188b werden folgende Angaben eingefügt:**

„§ 188c IT-gestützter Abgleich; Datenanalyse“

„§ 188d Durchführung des IT-gestützten Abgleichs und der Datenanalyse“

**d) Nach der Angabe zu § 195a werden folgende Angaben eingefügt:**

„§ 195b Nachträgliche Fernidentifizierung“

„§ 195c Durchführung der nachträglichen Fernidentifizierung“

**e) Die Angabe zu § 201b erhält folgende Fassung:**

„§ 201b Elektronische Aufenthaltsüberwachung bei Gefahren für wichtige Rechtsgüter“

**f) Die Angabe zu § 201c erhält folgende Fassung:**

„§ 201c Elektronische Aufenthaltsüberwachung bei terroristischen Gefahren“

**g) Nach der Angabe zu § 201c wird folgende Angabe eingefügt:**

„§ 201d Anordnung der elektronischen Aufenthaltsüberwachung“

**h) Die Angabe zu § 205 erhält folgende Fassung:**

„§ 205 Behandlung in Gewahrsam genommener Personen“

**i) Nach der Angabe zu § 205 wird folgende Angabe eingefügt:**

„§ 205a Richterliche Entscheidung bei Gewahrsam; rechtsanwaltliche Vertretung“

**2. § 181 Absatz 5 wird wie folgt gefasst:**

„(5) Wird eine Person aufgrund des Absatzes 4 Satz 2 festgehalten, ist § 205a entsprechend anzuwenden.“

**3. § 184 wird wie folgt gefasst:**

**„§ 184**
**Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an allgemein zugänglichen Orten**

(1) Bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, können personenbezogene Daten erhoben werden, wenn Tatsachen dafür sprechen, dass von den Betroffenen Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten begangen werden. Der offene Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen ist nur gegen die in den §§ 218 und 219 genannten Personen zulässig.

(2) Allgemein zugängliche Flächen dürfen mittels Bildübertragung beobachtet werden, soweit dies zur Aufgabenerfüllung nach § 162 erforderlich ist. Gleiches gilt für Räume, die nicht der Wohnung dienen, und auf befriedetem Besitztum zu einer Zeit, in der der Raum oder das befriedete Besitztum bestimmungsgemäß für die Allgemeinheit geöffnet ist.

(3) Offene Bild- und Tonaufnahmen oder -aufzeichnungen von Personen sind auf und an allgemein zugänglichen Flächen sowie in Räumen und auf befriedetem Besitztum im Sinne von Absatz 2 Satz 2 zulässig, wenn

1. dies zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich ist,

2. Tatsachen die Annahme rechtfertigen, dass an dem Ort Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten begangen werden oder

3. für die Orte die Voraussetzungen des § 181 Absatz 1 Nummer 1 bis 3 vorliegen.

Aufnahmen und Aufzeichnungen im Sinne des Satzes 1 an den in Satz 1 Nummer 3 bezeichneten Orten darf nur die Polizei anfertigen. Die Anordnungsvoraussetzungen gemäß Satz 1 Nummer 1 bis 3 sind schriftlich zu dokumentieren. Maßnahmen nach Satz 1 sind örtlich auf den erforderlichen Bereich zu beschränken und auf sechs Monate zu befristen. Eine Verlängerung ist nur zulässig, sofern die Anordnungsvoraussetzungen weiter vorliegen.

(4) Zum Schutz einer Polizeivollzugsbeamtin oder eines Polizeivollzugsbeamten oder eines Dritten kann die Polizei bei polizeilichen Maßnahmen nach diesem Gesetz oder anderen Rechtsvorschriften auf allgemein zugänglichen Flächen sowie in Räumen und auf befriedetem Besitztum im Sinne von Absatz 2 Satz 2 erforderlichenfalls offene Bild- und Tonaufnahmen oder -aufzeichnungen anfertigen.

(5) Bei den Maßnahmen nach Absatz 1 bis 3 dürfen automatisierte Anwendungen zur Datenverarbeitung zur Erkennung und Auswertung von Bewegungsmustern verwendet werden, die auf Handlungen hindeuten, mit welchen Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person beeinträchtigt werden. Sofern Muster nach Satz 1 erkannt werden, ist unverzüglich durch qualifizierte Beschäftigte der Polizei zu prüfen, ob eine Gefahr für die in Satz 1 genannten Rechtsgüter vorliegt. Liegt eine Gefahr für Rechtsgüter gemäß Satz 2 vor, darf zur Unterstützung gefahrenabwehrender Maßnahmen eine automatisierte Nachverfolgung der für die Gefahr verantwortlichen Person durch ihre Kennzeichnung in den vorliegenden Bildübertragungen, -aufnahmen oder -aufzeichnungen erfolgen. Zur Kennzeichnung nach Satz 3 sind vorrangig nicht körperliche Merkmale zu verwenden; eine automatisierte Identifizierung der gekennzeichneten Person anhand biometrischer Merkmale ist nach dieser Vorschrift nicht zulässig. Wird für eine Maßnahme nach Satz 1 oder 3 ein Hochrisiko-KI-System im Sinne der Verordnung (EU) 2024/1689[1] verwendet, muss die Polizei die Betreiberpflichten nach Artikel 26 Absatz 1 bis 6 sowie Absatz 9 und 12 der Verordnung (EU) 2024/1689 erfüllen. Im Falle des Satzes 5 gelten für die Unterrichtungspflicht nach Artikel 26 Absatz 11 der Verordnung (EU) 2024/1689 die Vorschriften des § 186 Absatz 7 und 8 entsprechend.

(6) Die nach dieser Vorschrift angefertigten Bild- und Tonaufzeichnungen sowie sonstige dabei gewonnene personenbezogene Daten sind spätestens einen Monat nach ihrer Erhebung zu löschen oder zu vernichten; die nach Absatz 5 erlangten Bewegungsmuster

1 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).

werden nicht gespeichert. Abweichend von Satz 1 dürfen Bild- und Tonaufzeichnungen länger gespeichert werden, soweit

1. sie zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten benötigt werden,

2. Tatsachen dafür sprechen, dass die Person künftig vergleichbare Straftaten oder Straftaten im Sinne des § 179 Absatz 2 begehen wird und die Speicherung zur Aufgabenerfüllung erforderlich ist,

3. eine Überprüfung der Rechtmäßigkeit der polizeilichen Maßnahme zu erwarten ist.

Die Löschung und die zweckändernde Verarbeitung der Bild- und Tonaufzeichnungen sind zu dokumentieren.

(7) Maßnahmen nach Absatz 1 bis 5 dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen sind. Auf den Umstand einer offenen Datenerhebung bei Maßnahmen nach den Absätzen 1 bis 4 ist in geeigneter Weise hinzuweisen. Auf die Verwendung einer automatisierten Anwendung im Sinne von Absatz 5 ist gesondert hinzuweisen.“

**4. Nach § 184a werden folgende §§ 184b und 184c eingefügt:**

**„§ 184b**
**Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen**

(1) Zur Ergänzung eines vorhandenen Sachverhalts darf die Polizei automatisiert in Echtzeit die Identität einer Person mit einer auf Bild- und Tonaufnahmen oder -aufzeichnungen im Sinne von § 184 Absatz 1 und 3 erkennbaren Person anhand biometrischer Merkmale bestätigen. Hierzu darf die Polizei aus Daten dieser Person, die sie im Rahmen ihrer Aufgaben erlangt hat, biometrische Referenzdaten gewinnen und diese mittels einer automatisierten Anwendung zur Datenverarbeitung in Echtzeit mit biometrischen Vergleichsdaten auf Übereinstimmungen abgleichen, die sie mittels einer automatisierten Anwendung von Personen erlangt, die auf den Bild- und Tonaufnahmen oder -aufzeichnungen erkennbar sind. Eine solche biometrische Echtzeit-Fernidentifizierung ist nur zulässig, soweit sie

1. im Hinblick auf die Ziele in Artikel 5 Unterabsatz 1 Buchstabe h Ziffer i der Verordnung (EU) 2024/1689 zur Abwehr einer Gefahr für Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person oder

2. im Hinblick auf die Ziele in Artikel 5 Unterabsatz 1 Buchstabe h Ziffer ii erste Alternative der Verordnung (EU) 2024/1689 oder

3. im Hinblick auf die Ziele in Artikel 5 Unterabsatz 1 Buchstabe h Ziffer ii zweite Alternative der Verordnung (EU) 2024/1689 zur Abwehr einer Gefahr für Leib, Leben oder Freiheit oder den Bestand oder die Sicherheit des Bundes oder eines Landes

unbedingt erforderlich ist. Die Anordnung muss unter Berücksichtigung der in Artikel 5 Absatz 2 der Verordnung (EU) 2024/1689 beschriebenen Abwägungsgesichtspunkte und der weiteren dort genannten Voraussetzungen für den Einsatz einer Anwendung zur biometrischen Echtzeit-Fernidentifizierung erfolgen. Satz 1 bis 4 sind auch anzuwenden, wenn kein KI-System im Sinne der Verordnung (EU) 2024/1689 verwendet wird.

(2) Eine Maßnahme nach Absatz 1 ist stets auf das zeitlich und örtlich unbedingt erforderliche Maß zu begrenzen. Sie darf nur durchgeführt werden, um auf den Bild- und Tonaufnahmen oder -aufzeichnungen

1. in Fällen des Absatzes 1 Satz 3 Nummer 1 eine der in Artikel 5 Unterabsatz 1 Buchstabe h Ziffer i der Verordnung (EU) 2024/1689 genannten Personen und

2. in Fällen des Absatz 1 Satz 3 Nummer 2 und 3 eine Person, von der die Gefahr ausgeht,

zu identifizieren.

(3) Eine Maßnahme nach Absatz 1 bedarf der vorherigen Genehmigung durch eine Richterin oder einen Richter. Die Genehmigung ist auf höchstens 7 Tage zu befristen. Soweit die Voraussetzungen weiterhin vorliegen, kann die Genehmigung verlängert werden, wobei jede Verlängerung auf höchstens 7 Tage zu befristen ist. Die richterliche Genehmigung und jede Verlängerung setzt einen schriftlichen und begründeten Antrag der Leiterin oder des Leiters des Landespolizeiamtes, des Landeskriminalamtes, einer Polizeidirektion oder durch von ihr oder ihm besonders beauftragte Personen des Polizeivollzugsdienstes voraus. Eine der in Satz 4 genannten Personen kann unter den Voraussetzungen und nach Maßgabe von Artikel 5 Absatz 3 Unterabsatz 1 Satz 2 der Verordnung (EU) 2024/1689 den Beginn der biometrischen Echtzeit-Fernidentifizierung ohne vorherige Genehmigung anordnen; in diesem Fall beantragt sie die nachträgliche richterliche Genehmigung unverzüglich, spätestens innerhalb von 24 Stunden. Wird die nachträgliche Genehmigung abgelehnt, gilt Artikel 5 Absatz 3 Unterabsatz 1 Satz 3 der Verordnung (EU) 2024/1689.

(4) Die Zuständigkeit und das Verfahren für richterliche Genehmigungen gemäß Absatz 3 bestimmen sich nach § 186 Absatz 3 Satz 1 und 2 sowie § 186 Absatz 6. Die zuständige Richterin oder der zuständige Richter hat über die Erteilung der Genehmigung nach Maßgabe von Artikel 5 Absatz 3 Unterabsatz 2 Satz 1 und 2 der Verordnung (EU) 2024/1689 zu entscheiden.

**§ 184c**
**Durchführung der Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen**

(1) Die zur Durchführung des Abgleichs gemäß § 184b Absatz 1 gewonnenen biometrischen Daten dürfen in polizeilichen Systemen nur bezogen auf den Zweck und den Anlasssachverhalt, für den sie erhoben wurden, verarbeitet werden; § 188a Absatz 1 und 2 ist ausgeschlossen. Das Ergebnis eines Abgleichs ist durch zwei qualifizierte Beschäftigte der Polizei zu überprüfen und zu bestätigen, bevor weitere polizeiliche Maßnahmen getroffen werden. Soweit weitere polizeiliche Maßnahmen getroffen werden, ist eine Speicherung des Ergebnisses des Abgleichs, das zu diesen Maßnahmen Anlass gibt, einschließlich der zur Erlangung dieses Abgleichergebnisses verwendeten Daten, zulässig. Im Übrigen sind nach Abschluss der Maßnahme alle gewonnenen biometrischen Daten und alle weiteren durch den Abgleich erlangten personenbezogenen Daten unverzüglich zu löschen. Die Vorgaben dieses Absatzes sind durch organisatorische und technische Vorkehrungen zu sichern.

(2) Die Person, die gemäß § 184b Absatz 2 Satz 2 identifiziert werden sollte, ist über die Durchführung der Echtzeit-Fernidentifizierung durch die Polizei zu benachrichtigen, sobald dies ohne Gefährdung des Zweckes der weiteren Datenverarbeitung möglich ist. § 186 Absatz 7 Satz 3 sowie Satz 5 bis 9 und Absatz 8 gelten entsprechend.

(3) Der Zugang zu der Anwendung, mit der Maßnahmen nach § 184b umgesetzt werden, ist auf bestimmte diesbezüglich qualifizierte Beschäftigte der Polizei beschränkt und unterliegt einer Zugriffskontrolle. Über die in § 186c vorgeschriebene Protokollierung hinaus sind die eingesetzte automatisierte Anwendung zur Datenverarbeitung und die Beschäftigten der Polizei, welche die Maßnahme durchführen, zu erfassen. Die Mitteilungspflichten nach Artikel 5 Absatz 4 der Verordnung (EU) 2024/1689 obliegen dem Landespolizeiamt. Das für Inneres zuständige Ministerium kann die technisch-organisatorischen Einzelheiten

1. zur Umsetzung und Absicherung der Vorgaben nach Absatz 1 zur Zweckbindung, Überprüfung des Abgleichergebnisses, Speicherung und Löschung,

2. zur Zugangsberechtigung, Zugangskontrolle und Protokollierung nach Satz 1 und Satz 2 und

3. zur Umsetzung der Mitteilungspflichten gemäß Satz 3

in einer Verwaltungsvorschrift regeln. Die Verwaltungsvorschrift ist im Benehmen mit der oder dem Landesbeauftragen für Datenschutz zu erlassen und zu veröffentlichen.“

**5. In § 186b Absatz 2 Satz 1 wird die Angabe „zu protokollierenden Maßnahmen.“ ersetzt durch die Angabe „zu protokollierenden Maßnahmen; ausgenommen von der Berichtspflicht sind Maßnahmen nach § 188c Absatz 1.“**

**6. In § 186c Absatz 1 wird der einleitende Teilsatz wie folgt gefasst:**

„Bei Durchführung einer Maßnahme nach § 180a Absatz 2 und 4, §§ 184b, 185, 185a, 185b, 185c, 188c, 195a und 195b sind zu protokollieren:“

**7. Nach § 188b werden folgende §§ 188c und 188d eingefügt:**

„**§ 188c**
**IT-gestützter Abgleich; Datenanalyse**

(1) Die Polizei darf nach Maßgabe des § 188a Absatz 1 und 2 und des § 479 Absatz 2 Satz 2 Nummer 1 und 2 der Strafprozessordnung zur Ergänzung eines vorhandenen Sachverhalts personenbezogene Daten für die Dauer der Bearbeitung der Sachverhalte zweckgebunden zusammenführen, um anhand zielgerichteter Suchkriterien Übereinstimmungen zwischen diesen Daten festzustellen (IT-gestützter Abgleich). Dabei dürfen nur personenbezogene Daten verwendet werden, die durch gezielte Abfragen aus den in Absatz 3 Satz 1 und Absatz 5 genannten Quellen erlangt werden.

(2) Nach Maßgabe von § 188a Absatz 1 und 2 und § 479 Absatz 2 Satz 2 Nummer 1 und 2 der Strafprozessordnung darf die Polizei darüber hinaus in polizeilichen Dateisystemen gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenverarbeitung zu den in den Absätzen 3 und 4 beschriebenen Zwecken anlassbezogen zusammenführen und anschließend zur Gewinnung neuer Erkenntnisse verarbeiten (Datenanalyse). Eine Verarbeitung des zusammengeführten Datenbestandes zu anderen Zwecken ist ausgeschlossen.

(3) Eine Datenanalyse, die beschränkt ist auf personenbezogene Daten aus Vorgangs- und Fallbearbeitungssystemen, polizeilichen Auskunfts-, Kommunikations-, Einsatzleit- und Einsatzdokumentationssystemen sowie Asservaten und anderen Beweismitteln, ist zulässig, wenn

1. bestimmte Tatsachen die Annahme rechtfertigen, dass eines der in Satz 2 genannten Rechtsgüter innerhalb eines absehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierten Weise durch einen Angriff von erheblicher Intensität oder Auswirkung gefährdet wird, und die Datenanalyse erforderlich ist, um einen Schaden von den Rechtsgütern abzuwenden, oder

2. die Datenanalyse der Verhütung von Straftaten dient, die ein in Satz 2 genanntes Rechtsgut schützen, soweit die Voraussetzungen nach Nummer 1 vorliegen, weil aufgrund tatsächlicher Anhaltspunkte innerhalb eines übersehbaren Zeitraums mit weiteren gleichgelagerten Straftaten zu rechnen ist.

Eine Datenanalyse im Sinne des Satzes 1 muss dem Schutz folgender Rechtsgüter dienen:

1. Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person, Bestand oder Sicherheit des Bundes oder eines Landes;

2. die Menschenwürde, sofern tatsächliche Anhaltspunkte für einen den öffentlichen Frieden bedrohenden Angriff im Sinn von § 130 Absatz 1 des Strafgesetzbuches vorliegen;

3. Umwelt, Eigentum oder Vermögenswerte, sofern tatsächliche Anhaltspunkte für eine drohende gewerbsmäßig oder bandenmäßig begangene Schädigung dieser Rechtsgüter vorliegen, die geeignet ist, den Rechtsfrieden in erheblicher Weise zu stören.

(4) Eine Datenanalyse, in die personenbezogene Daten aus sämtlichen Dateisystemen der Polizei und automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, einbezogen werden dürfen, ist zur Abwehr einer Gefahr für die in Absatz 3 Satz 2 Nummer 1 genannten Rechtsgüter zulässig. Im Fall der Verarbeitung personenbezogener Daten, die durch den Einsatz technischer Mittel in Wohnungen erhoben wurden, muss eine dringende Gefahr vorliegen. § 100e Absatz 6 Nummer 2 der Strafprozessordnung ist zu berücksichtigen.

(5) In einen IT-gestützten Abgleich oder eine Datenanalyse dürfen Datensätze aus gezielten Abfragen aus gesondert geführten staatlichen Registern, aus polizeilich nutzbaren Auskunfts- und Informationssystemen und aus von Dritten geführten Datenbeständen sowie einzelne gesondert gespeicherte Datensätze aus Internetquellen einbezogen werden, wenn dies zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist. Dasselbe gilt bei einem IT-gestützten Abgleich und einer Datenanalyse gemäß Absatz 3 für Datenbestände, die alle in einer Funkzelle anfallenden Verkehrsdaten enthalten.

(6) Für einen IT-gestützten Abgleich und eine Datenanalyse in den Fällen von Absatz 3 ist die Verarbeitung von personenbezogenen Daten, die durch den Einsatz technischer Mittel in Wohnungen oder durch verdeckten Zugriff auf informationstechnische Systeme gewonnen wurden, ausgeschlossen. Für Maßnahmen nach dieser Vorschrift (§ 188c) sind ausgeschlossen:

1. die Verarbeitung biometrischer Daten;

2. die Verwendung selbstlernender Systeme;

3. ein unmittelbarer automatisierter Abgleich von personenbezogenen Daten aus Internetdiensten.

(7) Durch eine Datenanalyse darf ein Profil über das Verhalten einer Person nur dann erstellt werden, wenn Tatsachen die Annahme rechtfertigen, dass diese Person für die Gefahr verantwortlich ist und das Verhaltensprofil zur Abwehr der Gefahr nach Absatz 3 Satz 1 Nummer 1 oder Absatz 4 oder zur Verhütung der Straftat nach Absatz 3 Satz 1 Nummer 2 erforderlich ist. Im Falle einer Datenanalyse nach Absatz 3 darf das Verhaltensprofil höchstens den Zeitraum von einer Woche umfassen. Die Erstellung automatisierter personenbezogener Bewertungen über die Gefährlichkeit oder andere Merkmale von Personen auf Grundlage statistischer oder algorithmischer Verfahren ist unzulässig.

(8) Einen IT-gestützten Abgleich kann eine Polizeivollzugsbeamtin oder ein Polizeivollzugsbeamter anordnen; die Anordnung ist zu begründen und die Begründung zu dokumentieren. Die Datenanalyse wird

1. in den Fällen des Absatzes 3 durch die Polizei nach Maßgabe von § 186 Absatz 2 und
2. in den Fällen des Absatzes 4 nach Maßgabe von § 186 Absatz 1 richterlich

angeordnet. Soll bei einer Datenanalyse ein Profil zum Verhalten einer Person nach Absatz 7 erstellt werden, muss dies in der Anordnung ausdrücklich zugelassen werden. Für die Anordnung der Datenanalyse nach Satz 2 gelten § 186 Absatz 3 Satz 1, 2, 4 und 5, Absatz 4 sowie Absatz 6 entsprechend.

**§ 188d**
**Durchführung des IT-gestützten Abgleichs und der Datenanalyse**

(1) Personenbezogene Daten, die für eine Maßnahme nach § 188c zusammengeführt werden sollen, müssen nach § 188b Absatz 1 gekennzeichnet sein. § 188b Absatz 1 Satz 3 Halbsatz 1 gilt mit der Maßgabe, dass die Kennzeichnung zumindest das Mittel der Datenerhebung sowie die Kategorie der von der Datenverarbeitung betroffenen Person einschließen muss. Sind auch die Informationen im Sinne des Satzes 2 nicht bekannt, dürfen die personenbezogenen Daten einbezogen werden, wenn nach besonderer Prüfung keine Zweifel an ihrer Verwertbarkeit bestehen.

(2) Die Verarbeitung der zusammengeführten personenbezogenen Daten nach § 188c muss auf Suchkriterien basieren, die auf den jeweiligen Anlass der Maßnahme zurückgeführt werden können. Es muss gewährleistet sein, dass personenbezogene Daten gestaffelt nach Kategorien (§ 188b Absatz 1 Nummer 2) verarbeitet werden, die die Rolle der betroffenen Person im für die Speicherung anlassgebenden Sachverhalt beschreiben; dabei ist so vorzugehen, dass zunächst Daten solcher Kategorien ausgewertet werden, denen eine für die Speicherung anlassgebende Rechtsgutsgefährdung oder -verletzung zugerechnet wird, bevor auf andere Kategorien zugegriffen wird.

(3) Die Nachvollziehbarkeit des verwendeten automatisierten Verfahrens zur Datenverarbeitung muss sichergestellt sein. Algorithmen, deren Regeln gruppenbezogenen Merkmalen im Sinne des Artikels 3 Absatz 3 des Grundgesetzes folgen, ohne dass dies durch den Zweck der Datenanalyse gerechtfertigt ist, dürfen nicht verwendet werden.

(4) Der Zugang zu der Anwendung, mit der Maßnahmen nach § 188c umgesetzt werden, ist auf bestimmte diesbezüglich qualifizierte Beschäftigte der Polizei beschränkt und unterliegt einer Zugriffskontrolle. Über die in § 186c vorgeschriebene Protokollierung hinaus sind die eingesetzte automatisierte Anwendung zur Datenverarbeitung und die Beschäftigten der Polizei, welche die Maßnahme durchführen, zu erfassen. Wird ein Hochrisiko-KI-System im Sinne der Verordnung (EU) 2024/1689 verwendet, muss die Polizei außerdem die Betreiberpflichten nach Artikel 26 Absatz 1 bis 6 sowie Absatz 9 und 12 der Verordnung (EU) 2024/1689 erfüllen.

(5) Die zum Zwecke der Datenanalyse nach Maßgabe von § 188c anlassbezogen zusammengeführten personenbezogenen Daten dürfen als Datenbestand nicht länger vorgehalten werden, als dies für den Zweck der Datenanalyse gemäß § 188c Absatz 3 oder 4 erforderlich ist. Sind die personenbezogenen Daten länger als 6 Monate zusammengeführt, ist regelmäßig, wenigstens aber alle 3 Monate die weitere Erforderlichkeit der Zusammenführung nach Satz 1 zu prüfen.

(6) Werden durch die Datenanalyse über eine Person neue Erkenntnisse erlangt, ist diese Person von der Polizei zu benachrichtigen, sobald dies ohne Gefährdung des Zweckes der weiteren Datenverarbeitung erfolgen kann. § 186 Absatz 7 Satz 3 sowie Satz 5 bis 9 und Absatz 8 gelten entsprechend. Wird ein Hochrisiko-KI-System im Sinne der Verordnung (EU) 2024/1689 verwendet, unterrichtet die Polizei mit der Benachrichtigung nach Satz 1 auch nach Maßgabe des Artikels 26 Absatz 11 der Verordnung (EU) 2024/1689 über die Verwendung des Hochrisiko-KI-Systems.

(7) Das für Inneres zuständige Ministerium bestimmt im Benehmen mit der oder dem Landesbeauftragten für Datenschutz durch eine zu veröffentlichende Verwaltungsvorschrift die technisch-organisatorischen Einzelheiten

1. zu den Sicherungen zur Einhaltung der Zweckbindung der verarbeiteten personenbezogenen Daten, einschließlich der Kennzeichnung nach Absatz 1,

2. zur Festlegung der Suchkriterien für die Verarbeitung der zusammengeführten Daten und zur Struktur des Verarbeitungsprozesses nach Absatz 2,

3. zur Gewährleistung der Nachvollziehbarkeit und Kontrolle des automatisierten Verfahrens zur Datenverarbeitung nach Absatz 3,

4. zur Zugangsberechtigung, Zugangskontrolle und Protokollierung nach Absatz 4 sowie zur Umsetzung und Absicherung der Betreiberpflichten der Verordnung (EU) 2024/1689 und

5. zur Speicherdauer des zusammengeführten Datenbestandes und deren Überprüfung nach Absatz 5.“

**8. § 192 wird wie folgt geändert:**

**a) Nach Absatz 3 wird folgender neuer Absatz 4 eingefügt:**

„(4) Für den Informationsaustausch im Anwendungsbereich der Richtlinie (EU) 2023/977[2] gelten Absatz 2 und 3, soweit er nicht über das Bundeskriminalamt als zentrale Kontaktstelle abgewickelt wird. Das für Inneres zuständige Ministerium wird ermächtigt, die Vor-

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).

gaben der Richtlinie (EU) 2023/977 für den Informationsaustausch im Sinne des Satzes 1 durch Rechtsverordnung zu regeln."

**b) Absatz 4 wird zu Absatz 5.**

**9. § 195 wird wie folgt geändert:**

**a) In Absatz 1 wird die Angabe „§ 179 Abs. 2 Nr. 2 Buchst. a" durch die Angabe „§ 179 Absatz 2 Nummer 1" ersetzt.**

**b) Absatz 2 wird wie folgt gefasst:**

„(2) Die Polizei darf einen Abgleich nach Absatz 1 auch anhand biometrischer Daten durchführen, die sie zu diesem Zweck aus Daten gewinnt, die aus anderem Anlass rechtmäßig in polizeilichen Datei- und Informationssystemen gespeichert wurden. Ein solcher Abgleich darf nur durchgeführt werden,

a) um die Identität zwischen einer bestimmten Person, von der entweder eine Gefahr für die öffentliche Sicherheit ausgeht oder die vor einer erheblichen Gefahr zu schützen ist, und einer Person festzustellen, über die Daten in den polizeilichen Datei- und Informationssystemen rechtmäßig gespeichert wurden und

b) wenn der Abgleich zur Abwehr einer Gefahr im Sinne der Nummer 1 zwingend erforderlich ist.

Aus dem Einsatz technischer Mittel in Wohnungen oder durch den verdeckten Zugriff auf informationstechnische Systeme erlangte personenbezogene Daten dürfen für den Abgleich nach Satz 1 nicht herangezogen werden; § 188a Absatz 3 bleibt unberührt. Die Anordnung der Maßnahme ist zu begründen und die Begründung zu dokumentieren. § 195b Absatz 2 Satz 3 und 195c Absatz 1 und 3 gelten entsprechend; wird für den Abgleich nach Satz 1 ein Hochrisiko-KI-System im Sinne der Verordnung (EU) 2024/1689 verwendet, ist auch § 195c Absatz 2 entsprechend anzuwenden."

**10. Nach § 195a werden folgende §§ 195b und 195c eingeführt:**

**„§ 195b**
**Nachträgliche Fernidentifizierung**

(1) Zur Ergänzung eines vorhandenen Sachverhalts darf die Polizei automatisiert die Identität einer Person mit einer in öffentlich zugänglichen Daten des Internet erkennbaren Person anhand biometrischer Merkmale bestätigen. Hierzu darf die Polizei aus Daten dieser Person, die sie im Rahmen ihrer Aufgaben erlangt hat, biometrische Referenzdaten gewinnen und diese mittels einer automatisierten Anwendung zur Datenverarbeitung mit nach Satz 3 gewonnenen biometrischen Vergleichsdaten auf Übereinstimmungen abgleichen. Zur Durchführung des Abgleichs nach Satz 2 darf die Polizei öffentlich

zugängliche personenbezogene Daten aus dem Internet mittels einer automatisierten Anwendung verarbeiten und aus diesen die biometrischen Vergleichsdaten gewinnen. Eine biometrische Fernidentifizierung nach dieser Vorschrift ist nur zulässig, soweit sie zur Abwehr einer Gefahr für Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person oder für den Bestand oder die Sicherheit des Bundes oder eines Landes unbedingt erforderlich ist. Nicht zulässig ist eine Fernidentifizierung mittels biometrischer Daten, die aus im Internet in Echtzeit übertragenen und veröffentlichten Video-, Audio- oder Bilddateien gewonnen werden.

(2) Eine Maßnahme nach Absatz 1 darf nur durchgeführt werden, um in den öffentlich zugänglichen Daten eine Person zu identifizieren, von der die Gefahr gemäß Absatz 1 Satz 4 ausgeht oder deren in Absatz 1 Satz 4 genannte Rechtsgüter gefährdet sind. Ihre Durchführung ist auch zulässig, wenn Dritte unvermeidbar betroffen sind. Wird für eine Maßnahme nach Absatz 1 ein Hochrisiko-KI-System im Sinne der Verordnung (EU) 2024/1689 verwendet, müssen zusätzlich zu den Voraussetzungen des Absatzes 1 die Voraussetzungen gemäß Artikel 26 Absatz 10 Unterabsatz 3 der Verordnung (EU) 2024/1689 erfüllt sein.

(3) Die Durchführung einer Maßnahme nach dieser Vorschrift darf nur auf Antrag durch die Leiterin oder den Leiter des Landespolizeiamtes, des Landeskriminalamtes, einer Polizeidirektion oder durch von ihr oder ihm besonders beauftragte Personen des Polizeivollzugsdienstes richterlich angeordnet werden. § 186 Absatz 1 Satz 2 bis 5 und Absatz 3 Satz 1, 2, 4 und 5, Absatz 4 sowie Absatz 6 sind entsprechend anzuwenden.

(4) Bei der Verarbeitung von öffentlich zugänglichen Daten ist zum Schutz des Kernbereichs privater Lebensgestaltung § 186a Absatz 1 und 5 anzuwenden.

**§ 195c**
**Durchführung der nachträglichen Fernidentifizierung**

(1) Die zur Durchführung des Abgleichs nach § 195b gewonnenen biometrischen Daten sowie die erlangten öffentlich zugänglichen personenbezogenen Daten dürfen in polizeilichen Systemen nur bezogen auf den Zweck und den Anlasssachverhalt, für den sie erhoben wurden, verarbeitet werden; § 188a Absatz 1 und 2 ist ausgeschlossen. Das Ergebnis eines Abgleichs ist, bevor weitere polizeiliche Maßnahmen getroffen werden, durch zwei Beschäftigte der Polizei zu überprüfen und zu bestätigen. Soweit weitere polizeiliche Maßnahmen getroffen werden, ist eine Speicherung des Ergebnisses des Abgleichs, das zu diesen Maßnahmen Anlass gibt, einschließlich der zur Erlangung dieses Abgleichergebnisses verwendeten Daten zulässig. Im Übrigen sind nach Abschluss der Prüfung gemäß Satz 2 alle gewonnenen biometrischen Daten, alle weiteren durch den Abgleich erlangten personenbezogenen Daten und alle zum Zwecke des Abgleichs erlangten öffentlich zugänglichen personenbezogenen Daten unverzüglich zu löschen. Die Vorgaben dieses Absatzes sind durch organisatorische und technische Vorkehrungen zu sichern.

(2) Die Person, die gemäß § 195b Absatz 2 Satz 1 identifiziert werden sollte, ist über die Durchführung der Maßnahme durch die Polizei zu benachrichtigen, sobald dies ohne Gefährdung des Zweckes der weiteren Datenverarbeitung möglich ist. § 186 Absatz 7 Satz 3 sowie Satz 5 bis 9 und Absatz 8 gelten entsprechend. Wird ein Hochrisiko-KI-System im Sinne der Verordnung (EU) 2024/1689 verwendet, unterrichtet die Polizei mit der Benachrichtigung nach Satz 1 auch nach Maßgabe des Artikels 26 Absatz 11 der Verordnung (EU) 2024/1689 über die Verwendung des Hochrisiko-KI-Systems.

(3) Der Zugang zu der Anwendung, mit der die Maßnahme umgesetzt wird, ist auf bestimmte diesbezüglich qualifizierte Beschäftigte der Polizei beschränkt und unterliegt einer Zugriffskontrolle. Über die in § 186c vorgeschriebene Protokollierung hinaus sind die eingesetzte automatisierte Anwendung zur Datenverarbeitung und die Beschäftigten der Polizei, welche die Maßnahme durchführen, zu erfassen. Wird ein Hochrisiko-KI-System im Sinne der Verordnung (EU) 2024/1689 verwendet, muss die Polizei außerdem die Betreiberpflichten nach Artikel 26 Absatz 1 bis 6, Absatz 9 und 10 Unterabsatz 5 sowie Absatz 12 der Verordnung (EU) 2024/1689 erfüllen; den Jahresbericht nach Maßgabe von Artikel 26 Absatz 10 Unterabsatz 6 der Verordnung (EU) 2024/1689 erstellt das Landespolizeiamt. Das für Inneres zuständige Ministerium kann die technisch-organisatorischen Einzelheiten

1. zur Umsetzung und Absicherung der Vorgaben nach Absatz 1 zur Zweckbindung, Überprüfung des Abgleichergebnisses, Speicherung und Löschung,

2. zur Zugangsberechtigung, Zugangskontrolle und Protokollierung nach Satz 1 und 2 und

3. in Fällen des Satzes 3 zur Umsetzung und Absicherung der Betreiberpflichten der Verordnung (EU) 2024/1689

in einer Verwaltungsvorschrift regeln. Die Verwaltungsvorschrift ist im Benehmen mit der oder dem Landesbeauftragen für Datenschutz zu erlassen und zu veröffentlichen.“

**11. § 200 wird wie folgt geändert:**

**a) Absatz 2 wird wie folgt gefasst:**

„(2) Einer festgehaltenen Person ist unverzüglich Gelegenheit zu geben, eine Angehörige oder einen Angehörigen oder eine Person ihres Vertrauens zu benachrichtigen. Die Regelungen des § 205 Absatz 2 sind entsprechend anzuwenden.“

**b) Absatz 4 wird wie folgt gefasst:**

„(4) § 205a gilt entsprechend.“

**12. In § 201a Absatz 6 wird der siebente Satz wie folgt gefasst:**

„Die Beratungsstelle im Sinne von Satz 1 Nummer 2 hat jedoch die Daten der Person, die eine Beratung abgelehnt hat, sowie die Umstände der Ablehnung ein Jahr lang zu speichern und der Polizei oder dem mit einem Antrag nach Absatz 4, nach § 201d oder nach dem Gewaltschutzgesetz befassten Gericht auf Aufforderung über diese Daten Auskunft zu erteilen."

**13. § 201b LVwG wird wie folgt gefasst:**

**„§ 201b**
**Elektronische Aufenthaltsüberwachung bei Gefahren für wichtige Rechtsgüter**

(1) Gegenüber einer Person kann angeordnet werden, sich ein technisches Mittel, mit dem der Aufenthaltsort dieser Person elektronisch überwacht werden kann, anlegen zu lassen, es ständig in betriebsbereitem Zustand am Körper bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen, wenn

1. bestimmte Tatsachen die Annahme rechtfertigen, dass Leben, Leib oder Freiheit einer Person oder deren sexuelle Selbstbestimmung innerhalb eines absehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise durch einen Angriff der zu überwachenden Person von erheblicher Intensität oder Auswirkung gefährdet sind und

2. die Überwachung des Aufenthaltsortes der Person, gegen die sich die Maßnahme richtet, unerlässlich ist, um einen Angriff im Sinne von Nummer 1 zu verhindern.

Die im Sinne von Satz 1 Nummer 1 gefährdete Person muss nicht notwendig individuell bestimmbar sein. Eine Maßnahme nach Satz 1 kann insbesondere zum Schutz einer bestimmten gefährdeten Person mit dem Ziel der Durchsetzung einer Maßnahme nach § 201a Absatz 1 Satz 1, Absatz 2 oder 4 oder § 201 Absatz 2 oder 3 angeordnet werden, wenn die Gefahr im Sinne von Satz 1 Nummer 1 sich für den Fall zu realisieren droht, dass die zu überwachende Person bestimmte Orte betritt, aufsucht oder sich dort aufhält oder mit einer gefährdeten Person zusammentrifft.

(2) Die Polizei darf mit Hilfe des von der überwachten Person bei sich geführten technischen Mittels automatisiert Daten über deren Aufenthaltsort sowie über etwaige Beeinträchtigungen der Datenerhebung verarbeiten. Darüber hinaus kann angeordnet werden, dass die erhobenen Daten zu einem Bewegungsbild verbunden werden dürfen, soweit dies zur Erfüllung des Überwachungszwecks erforderlich ist.

(3) Die Polizei darf mit Zustimmung einer im Sinne von Absatz 1 Satz 3 gefährdeten bestimmten Person Daten über deren Aufenthaltsort durch ein von dieser mitzuführendes technisches Mittel automatisiert erheben, speichern und mit den nach Absatz 2 erlangten Daten über den Aufenthaltsort der überwachten Person automatisiert abgleichen. Auf die Zustimmungserklärung der gefährdeten Person nach Satz 1 ist § 27 des Landesdatenschutzgesetzes vom 2. Mai 2018 (GVOBl. Schl.-H. S. 162) anzuwenden. Das Vorliegen

der Zustimmung der gefährdeten Person im Sinne des Satzes 1 ist in der richterlichen Anordnung gemäß § 201d anzugeben; wird die Zustimmung erst nachträglich erteilt, ist die überwachte Person hiervon unverzüglich in Kenntnis zu setzen. Der gefährdeten Person dürfen über das von ihr gemäß Satz 1 mitgeführte technische Gerät automatisiert Daten über den Aufenthaltsort der überwachten Person übermittelt werden, sobald die überwachte Person bestimmte Orte betritt, aufsucht oder sich dort aufhält oder sie sich der gefährdeten Person annähert.

(4) Die Maßnahmen nach Absatz 1 bis 3 sind zu dokumentieren. § 186a Absatz 7 ist entsprechend anzuwenden. Bei Datenerhebungen nach Absatz 2 und 3 ist nach dem Stand der Technik sicherzustellen, dass innerhalb der Wohnung der überwachten Person oder der gefährdeten Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden. Daten, die entgegen Satz 2 erhoben werden, dürfen nicht weiterverarbeitet werden und sind unverzüglich zu löschen; die Löschung ist zu dokumentieren.

(5) Werden die Daten im Sinne des Absatzes 2 und 3 nicht aufgrund des Absatzes 6 oder aufgrund anderer Rechtsvorschriften weiterverarbeitet, sind sie spätestens zwei Monate nach Beendigung der Maßnahme zu löschen. Bei jedem Abruf sind der Zeitpunkt, die abgerufenen Daten, die abrufende Person und der Grund des Abrufs zu protokollieren. Diese Protokolldaten sind nach zwölf Monaten zu löschen. Die Löschung von Daten nach diesem Absatz ist zu dokumentieren.

(6) Eine Weiterverarbeitung der nach Absatz 2 erlangten Daten der überwachten Person oder im Fall des Absatzes 3 der Daten der gefährdeten Person ist ohne deren jeweilige Einwilligung zulässig, wenn dies erforderlich ist

1. zur Abwehr einer Gefahr im Sinne des Absatzes 1 Satz 1 Nummer 1,

2. zur Feststellung von Verstößen gegen Maßnahmen nach §§ 201, 201a oder nach dem Gewaltschutzgesetz,

3. zur Verfolgung einer Straftat nach Absatz 7 oder nach dem Gewaltschutzgesetz,

4. zur Vorbereitung und Durchführung einer Abschiebung der überwachten Person, die im Verdacht steht, einen in § 54 Absatz 1 Nummer 1a des Aufenthaltsgesetzes genannten Straftatbestand erfüllt zu haben oder bei der tatsächliche Anhaltspunkte dafür bestehen, dass ein Ausweisungsinteresse im Sinne von § 54 Absatz 1 Nummer 2 bis 5 des Aufenthaltsgesetzes vorliegt, oder

5. zur Aufrechterhaltung der Funktionsfähigkeit des technischen Mittels.

Darüber hinaus ist die Weiterverarbeitung von nach Absatz 2 erlangten Daten zu Zwecken der Strafverfolgung unter den Voraussetzungen zulässig, unter denen nach Maßgabe der Strafprozessordnung retrograde Standortdaten erhoben werden dürfen.

(7) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer einer Anordnung nach Absatz 1 zuwiderhandelt und dadurch die ununterbrochene Feststellung seines Aufenthaltsortes verhindert. Die Tat wird nur auf Antrag der die Maßnahme beantragenden Behörde verfolgt.“

**14. § 201c LVwG wird wie folgt gefasst:**

**„§ 201c**
**Elektronische Aufenthaltsüberwachung bei terroristischen Gefahren**

(1) Eine Anordnung nach § 201b Absatz 1 Satz 1 ist auch gegenüber einer Person zulässig, deren individuelles Verhalten eine konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird und die Überwachung des Aufenthaltsortes dieser Person unerlässlich ist, um die Straftat zu verhindern. Eine terroristische Straftat im Sinne des Satzes 1 ist eine der in § 129a Absatz 1 oder Absatz 2 Nummer 1 bis 3 des Strafgesetzbuchs bezeichneten Straftaten, deren Versuch oder Begehung dazu bestimmt ist,

1. die Bevölkerung auf erhebliche Weise einzuschüchtern,

2. eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder

3. die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen,

und die durch die Art ihrer Begehung oder ihre Auswirkungen das Land Schleswig-Holstein, die Bundesrepublik Deutschland, ein anderes Bundesland oder einen anderen Staat oder eine internationale Organisation erheblich schädigen kann.

(2) Im Falle einer Anordnung nach Absatz 1 gilt § 201b Absatz 2 entsprechend. Im Hinblick auf Maßnahmen nach Absatz 1 und Datenerhebungen gemäß Satz 1 in Verbindung mit § 201b Absatz 2 sind § 201b Absatz 4 und 5 entsprechend anzuwenden. Eine Weiterverarbeitung der erhobenen Daten ohne Einwilligung der überwachten Person ist zulässig, wenn dies erforderlich ist

1. zur Verhütung oder zur Verfolgung einer terroristischen Straftat im Sinne des Absatzes 1 Satz 2,

2. zur Feststellung von Verstößen gegen Maßnahmen nach § 201,

3. zur Verfolgung einer Straftat nach Absatz 3 sowie

4. nach Maßgabe von § 201b Absatz 6 Satz 1 Nummer 4 und 5 sowie Absatz 6 Satz 2.

(3) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer einer Anordnung nach Absatz 1 zuwiderhandelt und dadurch die ununterbrochene Feststellung seines Aufenthaltsortes verhindert. Die Tat wird nur auf Antrag der die Maßnahme beantragenden Behörde verfolgt.“

**15. Nach § 201c wird folgender § 201d eingefügt:**

**„§ 201d Anordnung der elektronischen Aufenthaltsüberwachung**

(1) Eine Maßnahme nach § 201b oder § 201c und die mit ihr verbundene Datenverarbeitung wird auf Antrag der Polizei durch das nach § 186 Absatz 6 Satz 1 zuständige Gericht für höchstens drei Monate angeordnet. Das Gericht kann die Anordnung verlängern, soweit die Anordnungsvoraussetzungen weiterhin vorliegen; jede Verlängerung ist auf höchstens drei Monate zu befristen. Für das Verfahren finden die Vorschriften des Buches 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit nach Maßgabe der Absätze 2 bis 5 Anwendung. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(2) Vor Anordnung einer elektronischen Aufenthaltsüberwachung hat das Gericht die zu überwachende Person persönlich anzuhören. Erscheint die zu überwachende Person nicht zu dem Anhörungstermin, kann ihre sofortige Vorführung angeordnet werden. Das Gericht entscheidet hierüber durch nicht anfechtbaren Beschluss.

(3) Bei Gefahr im Verzug kann das Gericht eine einstweilige Anordnung der elektronischen Aufenthaltsüberwachung bereits vor der persönlichen Anhörung der zu überwachenden Person erlassen. Die persönliche Anhörung ist unverzüglich nachzuholen.

(4) Die Anordnung ergeht schriftlich. Bei Gefahr im Verzug kann die einstweilige Anordnung der elektronischen Aufenthaltsüberwachung mündlich ergehen; in diesem Fall ist die schriftliche Dokumentation unverzüglich nachzuholen. Für die Begründung der Entscheidung gilt § 186 Absatz 3 Satz 2 entsprechend; außerdem ist in ihr anzugeben, ob gegenüber der zu überwachenden Person auch eine Maßnahme nach § 201a Absatz 1 Satz 1, Absatz 2 oder 4 oder nach § 201 Absatz 2, 3 oder 4 erlassen wurde.

(5) Mit der Zustellung der Anordnung soll die Polizei nach § 168 Absatz 2 der Zivilprozessordnung beauftragt werden. Die Vollstreckung erfolgt gemäß § 245 Absatz 1 Nummer 1 durch die Polizei.“

**16. § 204 LVwG wird wie folgt gefasst:**

**„§ 204**
**Gewahrsam von Personen**

(1) Die Polizei kann eine Person nur in Gewahrsam nehmen, wenn dies

1. zu ihrem Schutz gegen eine Gefahr für Leib oder Leben erforderlich ist, insbesondere, weil sie sich erkennbar in einem die freie Willensbestimmung ausschließenden Zustand oder sonst in hilfloser Lage befindet,

2. unerlässlich ist, um die unmittelbar bevorstehende Begehung oder Fortsetzung einer Ordnungswidrigkeit von erheblicher Bedeutung für die Allgemeinheit oder einer Straftat zu verhindern; die Annahme der Begehung oder Fortsetzung einer Tat im Sinne des Halbsatzes 1 kann sich insbesondere darauf stützen, dass

a) die Person die Begehung der Tat angekündigt oder dazu aufgefordert hat oder Schriften oder andere Verkörperungen mit einer entsprechenden Ankündigung oder Aufforderung mit sich führt,

b) bei der Person Waffen, Werkzeuge oder sonstige Gegenstände aufgefunden werden und Tatsachen die Annahme rechtfertigen, dass diese Gegenstände zur Begehung der Tat bestimmt sind, oder ihre Begleitperson solche Gegenstände mit sich führt und sie den Umständen nach hiervon Kenntnis haben musste, oder

c) die Person bereits in der Vergangenheit mehrfach aus vergleichbarem Anlass bei der Begehung von Ordnungswidrigkeiten von erheblicher Bedeutung für die Allgemeinheit oder Straftaten als Störerin oder Störer in Erscheinung getreten ist und Tatsachen die Annahme rechtfertigen, dass weitere gleichartige Taten zu erwarten sind,

3. unerlässlich ist zur Abwehr einer Gefahr für Leib, Leben oder Freiheit oder die sexuelle Selbstbestimmung einer Person,

4. unerlässlich ist, um private Rechte zu schützen, und eine Festnahme und Vorführung der Person nach § 229 und § 230 Absatz 3 des Bürgerlichen Gesetzbuches zulässig ist,

5. unerlässlich ist,

a) um eine Maßnahme nach § 201 oder nach § 201a durchzusetzen, oder

b) weil die Person einer Anordnung nach § 201b nicht Folge leistet.

(2) Minderjährige, die sich der Obhut der Sorgeberechtigten entzogen haben, können in Gewahrsam genommen werden, um sie den Sorgeberechtigten oder dem Jugendamt zuzuführen.

(3) Eine Person, die aus dem Vollzug einer gerichtlich angeordneten Freiheitsentziehung entwichen ist oder sich sonst ohne Erlaubnis außerhalb der Vollzugseinrichtung aufhält, kann in Gewahrsam genommen werden und in die Vollzugseinrichtung zurückgebracht werden, aus der sie sich unerlaubt entfernt hat.

(4) Personen, die durch die örtliche Ordnungsbehörde auf Grundlage von § 252 Absatz 2 Nummer 2 erste Alternative zur Ausübung unmittelbaren Zwangs ermächtigt wurden, sind befugt, zur Ermöglichung einer Gewahrsamnahme

1. nach Absatz 1 Nummer 1, 2 und Nummer 4,
2. nach Absatz 1 Nummer 5, soweit der Gewahrsam der Durchsetzung von Maßnahmen nach § 201 dient, und

3. nach Absatz 2

die betroffene Person bis zum Eintreffen der Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten festzuhalten, soweit die Voraussetzungen des Gewahrsams jeweils vorliegen. Das Verbringen zur Dienststelle bleibt den Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten vorbehalten.

(5) Der Gewahrsam ist aufzuheben und die festgehaltene Person zu entlassen

1. unverzüglich, sobald der Grund hierfür weggefallen oder der Zweck erreicht ist,

2. unverzüglich, wenn die Fortdauer der Freiheitsentziehung durch richterliche Entscheidung für unzulässig erklärt wird,

3. spätestens bis zum Ende des Tages nach der Übernahme in den Gewahrsam, wenn nicht vorher die Fortdauer der Freiheitsentziehung durch richterliche Entscheidung nach § 205a angeordnet worden ist.

(6) Beruht der Gewahrsam auf einer richterlichen Entscheidung, hat diese die höchstzulässige Dauer der Freiheitsentziehung zu bestimmen. Sie darf jeweils nicht mehr als einen Monat betragen und kann insgesamt nur bis zu einer Gesamtdauer von zwei Monaten verlängert werden.“

**17. § 205 LVwG wird wie folgt gefasst:**

**„§ 205**
**Behandlung in Gewahrsam genommener Personen**

(1) Wird eine Person nach § 204 in Gewahrsam genommen, sind ihr unverzüglich der Grund der Maßnahme und die zulässigen Rechtsbehelfe bekanntzugeben, es sei denn, die Bekanntgabe wirkt sich für die Person nachteilig aus. Zu dieser Belehrung gehört der Hinweis, dass eine etwaige Aussage freiwillig erfolgt.

(2) Der in Gewahrsam genommenen Person ist unverzüglich Gelegenheit zu geben, einen Angehörigen oder eine Person ihres Vertrauens zu benachrichtigen, soweit dadurch der Zweck der Freiheitsentziehung nicht gefährdet wird. Die Polizei hat die Benachrichtigung zu übernehmen, wenn die in Gewahrsam genommene Person nicht in der Lage ist, von dem Recht nach Satz 1 Gebrauch zu machen und die Benachrichtigung ihrem mut-

maßlichen Willen nicht widerspricht. Ist die Gewahrsam genommene Person minderjährig, so ist in jedem Fall diejenige Person unverzüglich zu benachrichtigen, der die Sorge obliegt; ist für die in Gewahrsam genommene Person eine rechtliche Betreuerin oder ein rechtlicher Betreuer bestellt, so ist diese oder dieser zu benachrichtigen. § 432 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit bleibt unberührt.

(3) Die in Gewahrsam genommene Person soll gesondert, insbesondere ohne ihre Einwilligung nicht in demselben Raum mit Straf- oder Untersuchungsgefangenen untergebracht werden. Frauen und Männer sowie minderjährige und erwachsene Personen sind getrennt unterzubringen. Bei trans- oder intergeschlechtlichen Personen sowie nichtbinären Personen soll der geäußerte Wille bezüglich der Unterbringung berücksichtigt werden, sofern die Sicherheit und Ordnung der gewahrsamvollziehenden Einrichtung nicht gefährdet wird.

(4) Dauert die Freiheitsentziehung länger als drei Tage, sollen geeignete Maßnahmen zur Unterstützung der in Gewahrsam genommenen Person unverzüglich eingeleitet werden. Soweit geeignete Maßnahmen ihr Einverständnis voraussetzen, ist sie unverzüglich danach zu fragen und ein Einverständnis zu dokumentieren.

(5) Der in Gewahrsam genommenen Person dürfen nur solche Beschränkungen auferlegt werden, die zur Sicherung des Zwecks oder zur Aufrechterhaltung der Ordnung des amtlichen Gewahrsams notwendig sind.

(6) Soweit dies zum Schutz der in Gewahrsam genommenen Person oder von anwesenden Polizeivollzugsbeamtinnen oder Polizeivollzugsbeamten unerlässlich ist, kann sie in ihrem Gewahrsamsraum mittels Bildübertragung offen beobachtet werden. Unter den Voraussetzungen des Satzes 1 dürfen durch eine offene Anfertigung von Bild- und Tonaufzeichnungen auch personenbezogene Daten erhoben und verarbeitet werden. Befindet sich keine Polizeivollzugsbeamtin und kein Polizeivollzugsbeamter in dem Gewahrsamsraum, dürfen durch die offene Anfertigung von Bildaufzeichnungen personenbezogene Daten nur erhoben und weiterverarbeitet werden, soweit dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben der in Gewahrsam genommenen Person oder der höchstens kurzzeitigen Erforschung dieser Gefahr erforderlich ist. Die Datenerhebung ist für die betroffene Person wahrnehmbar und verständlich durch ein optisches oder akustisches Signal anzuzeigen. Der Schutz der Intimsphäre der in Gewahrsam genommenen Person ist zu wahren. Beginn, Ende, Umfang und Anlass der Maßnahmen nach Satz 1 und Satz 2 sind zu dokumentieren. § 184a Absatz 6 und 7 gilt entsprechend.

(7) Absatz 1 bis 6 gelten entsprechend, wenn eine Person durch die Polizei aufgrund anderer Rechtsvorschriften als § 204 festgehalten wird und für diesen Fall keine gesetzlichen Vorgaben zur Durchführung der Freiheitsentziehung und Behandlung der betroffenen Person bestehen.

(8) Wird der Gewahrsam im Wege der Amtshilfe in einer Justizvollzugsanstalt vollzogen, gelten die §§ 171 bis 175 und § 178 Absatz 2 Satz 1 des Strafvollzugsgesetzes vom 16. März 1976 (BGBl. I S. 581, 2088; 1977 I S. 436), zuletzt geändert durch Artikel 8 des Ge-

setzes vom 22. Dezember 2025 (BGBl. 2025 I Nr. 349) entsprechend. In diesem Fall übermittelt die Polizei der Justizvollzugsanstalt folgende Daten:

1. die das Verfahren führende Polizeidienststelle;
2. die Personen, die nach Absatz 2 benachrichtigt worden sind;

3. die gerichtliche Entscheidung zur Freiheitsentziehung und sonstige Maßnahmen, die zur Erfüllung der Aufgaben in Amtshilfe erforderlich sind;

4. sonstige Daten über die in Gewahrsam genommene Person, die für die Aufgabenerfüllung der Vollzugsanstalt erforderlich sind.“

**18. Nach § 205 LVwG wird folgender § 205a eingefügt:**

**„§ 205a**
**Richterliche Entscheidung bei Gewahrsam; rechtsanwaltliche Vertretung**

(1) Wird einer Person aufgrund von § 204 die Freiheit entzogen, ist durch die Polizei unverzüglich eine richterliche Entscheidung über Zulässigkeit und Fortdauer der Freiheitsentziehung herbeizuführen. Dies ist nicht erforderlich, wenn anzunehmen ist, dass die richterliche Entscheidung erst nach Wegfall des Grundes der polizeilichen Maßnahmen ergehen würde.

(2) Für die Entscheidung ist das Amtsgericht zuständig, in dessen Bezirk die Person festgehalten wird. Das Verfahren richtet sich nach den Vorschriften des Buches 1 und des Buches 7 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit.

(3) Zur richterlichen Entscheidung über die Fortdauer der Freiheitsentziehung über das Ende des Tages nach der Übernahme in den Gewahrsam hinaus bestellt das Gericht der in Gewahrsam genommenen Person, die noch keinen anwaltlichen Vertreter hat, von Amts wegen für die Dauer des Vollzugs eine anwaltliche Vertreterin oder einen anwaltlichen Vertreter als Bevollmächtigten.

(4) Ist die Freiheitsentziehung vor Erlass einer gerichtlichen Entscheidung beendet, kann die festgehaltene Person innerhalb eines Monats nach Beendigung der Freiheitsentziehung die Feststellung beantragen, dass die Freiheitsentziehung rechtswidrig gewesen ist. Der Antrag kann bei dem zuständigen Gericht schriftlich oder durch Erklärung zu Protokoll der Geschäftsstelle dieses Gerichts gestellt werden.

(5) Für Gerichtskosten gelten die Vorschriften des Gerichts- und Notarkostengesetzes vom 23. Juli 2013 (BGBl. I S. 2586), zuletzt geändert durch Artikel 6 des Gesetzes vom 10. Dezember 2025 (BGBl. 2025 I Nr. 320), entsprechend, soweit durch Rechtsvorschrift nichts anderes bestimmt ist. Für den Vergütungsanspruch eines nach Absatz 3 bestellten Rechtsanwalts gelten die Vorschriften des Rechtsanwaltsvergütungsgesetzes in der Fas-

sung der Bekanntmachung vom 15. März 2022 (BGBl. I S. 610), zuletzt geändert durch Artikel 14 des Gesetzes vom 8. Dezember 2025 (BGBl. 2025 I Nr. 318), entsprechend.“

**19. In § 258 Absatz 2 Nummer 4 wird im einleitenden Teilsatz nach der Angabe „einer Person, die“ die Angabe „in Gewahrsam, Verwahrung oder Haft genommen oder untergebracht worden ist (amtlicher Gewahrsam) und“ eingefügt.**

**Artikel 2**
**Inkrafttreten**

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.

Das vorstehende Gesetz wird hiermit ausgefertigt und ist zu verkünden.

Kiel,

Daniel Günther

Ministerpräsident

Magdalena Finke

Ministerin für Inneres, Kommunales, Wohnen und Sport

**Begründung:**

## A. Allgemeiner Teil

Dieser Gesetzentwurf verbindet unterschiedliche Vorhaben, Maßnahmen und Neugestaltungen im Gefahrenabwehrrecht Schleswig-Holsteins. Die neu geschaffenen Befugnisse zur biometrischen Fernidentifizierung (§§ 184b, 184c und §§ 195 Absatz 2, 195b, 195c LVwG-Entwurf) und zur automatisierten Datenanalyse (§§ 188c, 188d LVwG-Entwurf) sind moderne Formen des Datenabgleichs. Sie werden als besondere Mittel der Polizei zur Datenerhebung und Datenverarbeitung im Abschnitt „Öffentliche Sicherheit“ des Zweiten Teils des Landesverwaltungsgesetzes neu eingeführt. In diesem Kontext erfahren die Befugnisse für Videoaufzeichnungen im öffentlichen Raum (§ 184 LVwG-Entwurf) in einzelnen Punkten Änderungen. Mit den Vorschriften über den Polizeigewahrsam (§§ 204 bis 205a LVwG-Entwurf) wird dagegen ein tradierter Regelungsbereich umfassend novelliert und systematisch geschlossen. Schließlich erhält die elektronische Aufenthaltsüberwachung als ein relativ neues Instrument der Gefahrenabwehr eine veränderte Regelungsstruktur (§§ 201b bis 201d LVwG-Entwurf).

### I. Schaffung einer Rechtsgrundlage für die automatisierte Datenanalyse

Die automatisierte Datenanalyse und -auswertung ist im Grundsatz eine Form der Weiternutzung von verfügbaren personenbezogenen Daten. Ihr besonderes Potenzial liegt darin, große und komplexe Informationsstände zusammenzuführen und dadurch auswertbar zu machen. Von zentraler Bedeutung ist es dabei, die technischen Grenzen zu überwinden, die darin bestehen, dass Informationen häufig unstrukturiert, in unterschiedlichen Formaten und in disparaten Dateien gespeichert sind und damit nicht im gleichen Bearbeitungskontext simultan verfügbar sind. Ist in einem ersten Schritt dieses Zusammenführen der Daten vollzogen, können in einem zweiten Schritt mittels konkreter Suchvorgänge Strukturen, Handlungsmuster, Personengruppen sowie zeitliche, sachliche, organisatorische, personelle und situative Zusammenhänge sichtbar gemacht werden. Eingriffsintensive Formen der automatisierten Datenanalyse und -auswertung vermögen Strukturen, Muster und Zusammenhänge aufzuzeigen, die ein Mensch, auch wenn er Zugang zu allen diesen Informationen hätte, so nicht oder kaum hätte erkennen können.

**1.** Erste Befugnisse zur automatisierten Datenanalyse und -auswertung hatten 2018 beziehungsweise 2019 das Bundesland Hessen und die Freie und Hansestadt Hamburg geschaffen. Das Bundesverfassungsgericht (BVerfG) hat in Bezug auf diese Vorschriften in seiner Entscheidung (1 BvR 1547/19 pp.) vom 16. Februar 2023 (= BVerfGE 165, 363) die Bedingungen einer verfassungsrechtlichen Rechtfertigung grundlegend umrissen:

Das Eingriffsgewicht und die Rechtfertigungsanforderungen ergeben sich zunächst – nämlich soweit es um die Weiternutzung rechtmäßig erhobener Daten geht – aus den Grundsätzen der Zweckbindung und Zweckänderung. Maßgeblich ist insoweit das Gewicht des vorausgegangenen Datenerhebungseingriffs. Das Eingriffsgewicht der Datenanalyse oder -auswertung lässt sich aber nicht allein an diesem Maßstab beurteilen. Denn die Möglichkeit, durch den beschriebenen Mechanismus neue auf andere Weise

nicht oder kaum zu generierende Erkenntnisse zu gewinnen, stellt einen selbständig wirksamen Faktor bei der Beurteilung der Eingriffstiefe dar. Aus ihm sind weitere Rechtfertigungsanforderungen abzuleiten.

Wichtig ist in diesem Zusammenhang zu erkennen, dass das spezifische Eingriffsgewicht einer bestimmten automatisierten Datenanalyse oder -auswertung nicht stets gleich ist, sondern von der näheren Ausgestaltung der jeweiligen Befugnisnorm abhängt, vor allem von der Art und dem Umfang der verarbeiteten Daten und der zugelassenen Analyse- und Auswertungsmethode. Der Gesetzgeber hat es daher in der Hand, die Eingriffstiefe der Datenanalyse zu steuern.

**2.** Das BVerfG entwirft in der vorgenannten Entscheidung ein ganzes Spektrum an Faktoren zu Art und Umfang der verarbeiteten Daten (a. a. O. Rn. 78 bis 89) und zur Methode der Datenanalyse und -auswertung (a. a. O. Rn. 90 bis 102), die das Eingriffsgewicht der automatisierten Datenanalyse und -auswertung prägen. Je nach dem anhand dieser Kriterien zu messenden Gewichts des Eingriffs sind die Eingriffsvoraussetzungen auszuformen:

Liegt ein schwerwiegender Eingriff vor, wendet das BVerfG die für eingriffsintensive heimliche Überwachungsmaßnahmen entwickelten Maßstäbe an (a. a. O. Rn. 104 bis 106). Davon abzuschichten sind weniger gewichtige Eingriffe, bei denen eine Öffnung der Eingriffsvoraussetzungen in Bezug auf den Kreis der Schutzgüter und der Eingriffsschwelle gestattet ist (a. a. O. Rn. 107). Schließlich ist dann, wenn die einbeziehbaren Daten so reduziert und die möglichen Methoden von vornherein so eingeschränkt sind, dass die Erkenntnisse (wenngleich aufwendiger und langsamer) auch ohne automatisierte Anwendung (manuell) erlangt werden können, die Einhaltung des Grundsatzes der Zweckbindung der Maßstab für die Rechtfertigung des Grundrechtseingriffs (a. a. O. Rn. 108).

Entlang dieses Rasters sind die Eingriffsvoraussetzungen des § 188c LVwG-Entwurf konzipiert, sodass über die Absätze 1, 3 und 4 ein abgestuftes Instrumentarium an Maßnahmen beginnend bei der niedrigsten bis zur höchsten Eingriffstiefe entsteht. Daneben enthalten § 188c Absatz 5 bis 8 und § 188d LVwG-Entwurf flankierende Vorschriften zur Regulierung der Eingriffstiefe. Die letztgenannte Vorschrift ermächtigt überdies – in Übereinstimmung mit den Vorgaben des BVerfG zur Reichweite des Gesetzesvorbehalts (a. a. O. Rn. 115 bis 122) –, organisatorische und technische Einzelheiten in einer Verwaltungsvorschrift noch weiter zu konkretisieren.

## II. Schaffung von Rechtsgrundlagen zur biometrischen Fernidentifizierung

Die biometrische Fernidentifizierung bezeichnet eine Maßnahme, mit der eine Person ohne ihre aktive Einbeziehung und in der Regel aus der Ferne durch Abgleich ihrer biometrischen Daten mittels gespeicherter biometrischer Referenzdaten identifiziert wird. Dabei werden aus der Aufzeichnung der Stimme oder aus Bildern des Gesichts der Zielperson durch eine Software die charakteristischen Eigenschaften errechnet. Das Ergebnis dieser Berechnung, das sogenannte Template, wird mit anderen Templates abgegli-

chen, die auf gleiche Weise aus gespeicherten Stimmaufzeichnungen und Gesichtsbildern der Referenzdaten gewonnen wurden.

**1.** Dieser Gesetzentwurf normiert drei Formen der biometrischen Fernidentifizierung. Sie unterscheiden sich hinsichtlich der Referenzdatenquelle:

- Im Fall des § 195 Absatz 2 LVwG-Entwurf werden aus Daten zu Stimmen und Gesichtern, die bereits rechtmäßig in polizeilichen Systemen gespeichert sind, biometrische Daten gewonnen und miteinander abgeglichen.

- Für die biometrische Fernidentifizierung gemäß § 195b LVwG-Entwurf werden als Vergleichsdaten öffentlich zugängliche Daten verwendet, die die Polizei zu diesem Zweck zuvor in einem vorgelagerten Schritt mithilfe einer automatisierten Anwendung aus dem Internet erlangt hat.

- Bei § 184b LVwG werden für den Abgleich Live-Bild- und -Tonaufnahmen und -aufzeichnungen einer Videoüberwachung des öffentlichen Raums herangezogen.

Im letztgenannten Fall kann von einer Echtzeit-Identifizierung gesprochen werden, weil die Erfassung der biometrischen Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen. Demgegenüber lassen sich die beiden erstgenannten Formen als nachträgliche Fernidentifizierungen bezeichnen.

**2.** Wird für die Fernidentifizierung ein „KI-System“ im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz pp. (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj) – sogenannte KI-Verordnung – eingesetzt, sind die Vorgaben dieser Verordnung zu beachten. Dabei ist zu berücksichtigen, dass Systeme zur biometrischen Fernidentifizierung grundsätzlich als sogenannte Hochrisiko-KI-Systeme (gemäß Artikel 6 Absatz 2 in Verbindung mit Anhang III Nummer 1 Buchstabe a der KI-Verordnung) einzustufen sind. Aus dieser Einstufung folgen für die Polizei als Betreiber solcher Systeme besondere Pflichten (insbesondere Artikel 26 KI-Verordnung). Systeme zur biometrischen Echtzeit-Fernidentifizierung, die für Maßnahmen des § 184b LVwG zum Einsatz kommen, zählen zu den verbotenen Praktiken im Sinne der KI-Verordnung und sind nur unter den engen Voraussetzungen von Artikel 5 Unterabsatz 1 Buchstabe h und Absatz 2 bis 7 der Verordnung (EU) 2024/1689 zulässig.

**3.** Die Verordnung (EU) 2024/1689 schafft ein spezifisches Regelungsregime für den Einsatz von KI-Systemen. Dieses stellt jedoch nur einen Aspekt des rechtlichen Rahmens des polizeilichen Einsatzes von Instrumenten zur biometrischen Fernidentifizierung dar. Einen anderen zentralen Aspekt bilden die verfassungsrechtlichen Schranken für die Inanspruchnahme des Grundrechts auf informationelle Selbstbestimmung (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz/GG).

Zwei Punkte sind für die Ausgestaltung der Eingriffsbefugnisse verfassungsrechtlich von zentraler Bedeutung:

- Für die Ausgestaltung der Eingriffsvoraussetzungen ist von wesentlicher Bedeutung, dass dann, wenn als Referenzdaten Video- und Tonaufzeichnungen aus der Videoüberwachung des öffentlichen Raums herangezogen werden, automatisiert in großem Umfang personenbezogene Daten Unbeteiligter, also Personen, die keinen Bezug zur Gefahrenlage haben und für die die Maßnahme daher anlasslos ist, verarbeitet werden. Das gilt in gleicher Weise bei der Verwendung von öffentlich zugänglichen Daten zu Stimmen und Gesichtern, die aus dem Internet gewonnen werden. In beiden Fällen ist die Inanspruchnahme der Unbeteiligten zudem mehr als nur geringfügig; denn für jeden einzelnen Abgleich müssen die höchstpersönlichen Charakteristika der Stimme oder des Gesichts ermittelt und als Template gespeichert werden. Der Einsatz der grundrechtssensiblen Formen biometrischer Fernidentifizierung ist daher verfassungsrechtlich nur zu Abwehr konkreter Gefahren für hochrangige Rechtsgüter gerechtfertigt.

- Wegen der spezifischen Form der Datenverarbeitung im Fall der Fernidentifizierung sind besondere Schutzvorkehrungen zu treffen. Die aus den Stimmaufzeichnungen und Gesichtsbildern gewonnenen biometrischen Daten eines Menschen, beziehungsweise die entsprechenden Templates, sind nahezu unveränderlich und haben daher technisch das Potenzial, in vielfältiger Weise weitergenutzt zu werden. Diesem Risiko – das einen zentralen Kritikpunkt an Methoden zur biometrischen Fernidentifizierung darstellt – kann durch eine strenge Bindung der gewonnenen Daten an den Erhebungsanlass begegnet werden.

## III. Ausbau der Videoüberwachung im öffentlichen Raum

Die Echtzeit-Identifizierung nach § 184b LVwG-Entwurf greift als Referenzquelle für den biometrischen Abgleich auf die Daten einer Videoüberwachung von öffentlichen Räumen und Flächen zu, die auf Grundlage von § 184 LVwG erhoben werden. Im Kontext der Normierung der neuen Eingriffsbefugnis sind punktuell Anpassungen der Befugnis zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen im öffentlichen Raum angezeigt. Neben redaktionellen Änderungen stehen folgende Punkte im Vordergrund:

**1.** Die Voraussetzungen, unter denen bestimmte allgemein zugängliche oder für die Allgemeinheit geöffnete Bereiche überwacht werden können, werden ausgebaut. Über die bisher fokussierten Kriminalitäts- oder Gefahrenschwerpunkte hinaus werden alle sogenannten gefährlichen und gefährdeten Orte im Sinn von § 181 Absatz 1 Nummer 1 bis 3 LVwG einbezogen, z. B. auch besonders schützenswerte Objekte wie Versorgungs- oder Verkehrseinrichtungen. Außerdem wird dem Umstand Rechnung getragen, dass durch mobile Überwachungstechnik mittlerweile bei einer akuten Gefahrenlage im Einzelfall eine Videoüberwachung kurzfristig eingerichtet werden kann. Daher wird die Befugnis geschaffen, zur Abwehr einer (konkreten) Gefahr für die öffentliche Sicherheit anlassbezogen eine Videoüberwachung temporär einzurichten, auch wenn dieser Ort (noch) nicht durch Lageerkenntnisse als besonders gefährlich ausgewiesen ist.

**2.** Einer wichtigen technischen Entwicklung wird mit der neuen Rechtsgrundlage für den Einsatz automatisierter Anwendungen zur Mustererkennung gemäß § 184 Absatz 5 LV-

wG-Entwurf Rechnung getragen. Die entsprechende Software ist in der Lage, Video- und Audiodaten automatisiert zu erfassen und zu analysieren, um die erlangten Informationen nach Auffälligkeiten abzusuchen, die auf bestimmte Handlungen (z. B. Tumulte, Schlagbewegungen, Gegenstände) hindeuten, durch die Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person beeinträchtigt werden können. Diese Technik erhöht die Eignung der Videoüberwachung als Mittel der Gefahrenabwehr signifikant. Studien weisen darauf hin, dass eine manuelle Auswertung von Videodaten häufig deswegen nicht effektiv ist, weil die menschliche Aufmerksamkeit bei der Überwachung von Monitoren bereits nach kurzer Zeit signifikant abnimmt. Automatisierte Videoüberwachungssysteme können überdies sogenanntem „Social Sorting“ vorbeugen. Damit ist gemeint, dass Menschen das Attribut „gefährlich“ Vorgängen in Abhängigkeit von Ethnie oder Herkunft zuweisen. Am Ende steht allerdings in jedem Fall auch ein menschlicher Entscheider, der den von der Software als „auffällig“ markierten Vorgang bewerten und gegebenenfalls weitere Maßnahmen veranlassen muss. Eine hinreichende, auf die Aufgabe bezogene Qualifikation der Beschäftigten der Polizei, welche diese Aufgabe ausüben, ist zu gewährleisten.

## IV. Novellierung der Vorschriften über den Polizeigewahrsam

Der Gesetzentwurf gestaltet den Polizeigewahrsam neu. Neben einer Fortentwicklung der Vorschriften zur Durchführung des Gewahrsams (§ 205 LVwG-Entwurf) und zum Verfahren (§ 204 Absatz 5 und 6 sowie § 205a LVwG-Entwurf) stehen die Gewahrsamstatbestände gemäß § 204 Absatz 2 Nummer 2 und 3 LVwG-Entwurf im Zentrum der Reform.

**1.** Der Gewahrsamstatbestand gemäß § 204 Absatz 1 Nummer 2 LVwG erfasst de lege lata Fälle, in denen eine Ingewahrsamnahme einer Person unerlässlich ist, um die unmittelbar bevorstehende Begehung oder Fortsetzung „einer Straftat“ oder „einer Ordnungswidrigkeit von erheblicher Bedeutung für die Allgemeinheit“ zu verhindern. Der Gesetzentwurf kehrt lediglich die Reihenfolge der Tatbestandsmerkmale um, um im Wortlaut klarzustellen, dass sich die einschränkende Formulierung „von erheblicher Bedeutung für die Allgemeinheit“ nur auf die Unterbindung von Ordnungswidrigkeiten bezieht (vgl. nur Martens in PdK SH A-15, LVwG § 204 Anm. 4.1 m w. N.). Darüber hinaus wird der insoweit inhaltlich unveränderte Tatbestand um sogenannte legislative Prognosehilfen ergänzt. Das heißt, dass bestimmte Anknüpfungstatsachen ins Gesetz aufgenommen werden, auf welche die Prognose, dass eine Person eine Straftat begehen oder zu ihrer Begehung beitragen wird, insbesondere gestützt werden kann, nämlich

- das Bekenntnis zur Tat (§ 204 Absatz 1 Nummer 2 Buchstabe a),
- das Auffinden bestimmter Gegenstände (§ 204 Absatz 1 Nummer 2 Buchstabe b) und
- die Wiederholungsgefahr (§ 204 Absatz 1 Nummer 2 Buchstabe c).

Es handelt sich hierbei um Auslegungshilfen. Die legislativen Prognosehilfen stellen keine Regelbeispiele dar, die die Polizei oder den Richter binden oder eine Umkehr der Beweislast bewirken könnten. Ihr Vorteil besteht darin, das polizeiliche Handeln möglichst

zu vereinheitlichen und seine Messbarkeit und Vorhersehbarkeit zu erhöhen. Zugleich erfährt die Prognose im Einzelfall, die sich auf die gesetzlichen Anknüpfungstatsachen stützt, eine höhere Legitimität.

**2.** Mit § 204 Absatz 1 Nummer 3 LVwG-Entwurf wird ein neuer Gewahrsamstatbestand geschaffen. Dieser schließt eine Schutzlücke innerhalb der bestehenden Befugnisse, aufgrund derer im Einzelfall einer Person vorübergehend die Freiheit entzogen werden kann, wenn dies zur Abwehr erheblicher Gefahren für Rechtsgüter von Bürgerinnen und Bürgern geboten ist. Zu den bestehenden Befugnissen dieser Art sind, neben dem bereits genannten Gewahrsamstatbestand gemäß § 204 Absatz 1 Nummer 2 LVwG, die Unterbringung von Personen nach § 7 des Gesetzes zur Hilfe und Unterbringung von Menschen mit Hilfebedarf infolge psychischer Störungen (PsychHG) in Fällen, in denen aufgrund einer psychischen Störung bedeutende Rechtsgüter anderer erheblich gefährdet werden, sowie der Haftgrund der Wiederholungsgefahr nach § 112a der Strafprozessordnung (StPO) zu zählen.

Innerhalb des sich durch die genannten Normen ergebenden Regelungsgefüges bestehen im Einzelfall Schutzlücken, in denen der Staat seiner Schutzpflicht angesichts erheblicher Gefahren für besonders wichtige Rechtsgüter unter Umständen nicht gerecht werden kann:

- Die Unterbringung nach dem PsychHG knüpft die Freiheitsentziehung an eine ganz spezifische, medizinische Ursache an, nämlich die psychische Disposition der Störerin oder des Störers.

- § 112a StPO normiert einen Haftgrund mit präventiver Zielrichtung, der an verschiedene Voraussetzungen geknüpft ist. Die oder der Beschuldigte muss einer der enumerativ aufgeführten Anlasstaten dringend verdächtig sein, es muss die Gefahr bestehen, dass diese Person vor einer rechtskräftigen Verurteilung weitere erhebliche Straftaten gleicher Art begehen wird oder die Straftat fortsetzt, und die Haft muss zur Verhinderung dieser Wiederholungsgefahr erforderlich sein.
  Innerhalb der Vorschrift besteht eine Binnendifferenzierung zwischen zwei Konstellationen, die sich in Bezug auf die Anlasstat unterscheiden: Nur bei bestimmten Sexualdelikten sowie besonders schweren Formen der Nachstellung genügt der dringende Tatverdacht (§ 112a Absatz 1 Nummer 1 StPO). Bei anderen Anlasstaten muss eine wiederholte und fortgesetzte Begehung vorliegen, durch die die Rechtsordnung in schwerwiegender Weise beeinträchtigt wurde; außerdem muss die Straferwartung wegen der Anlasstat mehr als ein Jahr Freiheitsstrafe betragen (§ 112a Absatz 1 Nummer 2 StPO). Voraussetzung einer wiederholten Begehung ist, dass die oder der Beschuldigte mindestens zweimal dasselbe Strafgesetz verletzt hat. Dabei ist ausreichend, dass das Verfahren, in dem die Haftfrage zu prüfen ist, nur eine Anlasstat zum Gegenstand hat und die oder der Beschuldigte wegen mindestens einer weiteren Tat verurteilt worden ist oder anderweitig unter dringendem Tatverdacht verfolgt wird. Die Einschränkung des Haftgrundes auf Fälle der wiederholten Begehung führt dazu, dass er tendenziell auf Serien gleichartiger Taten ausgerichtet ist.

- Der Gewahrsamstatbestand nach § 204 Absatz 1 Nummer 2 LVwG erlaubt zwar die Ingewahrsamnahme zur Verhinderung von Straftaten und bestimmten Ordnungswidrigkeiten. Er setzt aber eine qualifizierte Gefahr solcher Taten voraus, nämlich dass diese unmittelbar bevorstehen. Das ist nur dann der Fall, wenn konkrete Anhaltspunkte dafür vorliegen, dass sich die Tat sofort oder in allernächster Zeit mit großer Wahrscheinlichkeit ereignen wird.

Droht für die besonders wichtigen Rechtsgüter Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung eine Gefahr, die nicht im Zusammenhang mit einer psychischen Störung steht, die von einer Person ausgeht, die nicht oder erst einmal mit einschlägigen Straftaten in Erscheinung getreten ist, und ist die Gefahrenlage noch nicht so weit fortgeschritten, dass die Rechtsgutsverletzung unmittelbar bevorsteht, gibt es de lege lata keine Möglichkeit, die Störerin oder den Störer in Gewahrsam zu nehmen, auch wenn dies das einzige geeignete Mittel zur Abwendung der Gefahr wäre. Diese Schutzlücke schließt der Gesetzentwurf durch den Gewahrsamstatbestand nach § 204 Absatz 1 Nummer 3 LVwG-Entwurf. Er ist mithin als Auffangtatbestand für Fallkonstellationen ausgestaltet, die aus dem dargestellten Regelungsgefüge herausfallen.

**3.** Das Regelungsziel wird umgesetzt, indem die Eingriffs- respektive Gefahrenschwelle abgesenkt wird. Der § 204 Absatz 1 Nummer 3 LVwG-Entwurf hat gegenüber § 204 Absatz 1 Nummer 2 LVwG reduzierte Voraussetzungen hinsichtlich zeitlicher Nähe und Wahrscheinlichkeit des Schadenseintritts. Ausreichend ist eine konkrete Gefahr, also die Standard-Eingriffsschwelle polizeilichen Handelns zum Beispiel im Rahmen der gefahrenabwehrrechtlichen Generalklausel. Eine solche Gefahr liegt vor, wenn nach allgemeiner Lebenserfahrung bei ungehindertem Verlauf des objektiv zu erwartenden Geschehens im Einzelfall mit hinreichender Wahrscheinlichkeit davon auszugehen ist, dass es zu einer Verletzung der Schutzgüter der öffentlichen Sicherheit oder Ordnung kommt. Angesichts der Schwere des Grundrechtseingriffs, der mit der Ingewahrsamnahme einhergeht, ist die Herabsenkung der Eingriffsschwelle und damit die Erweiterung des Gewahrsamstatbestands verfassungsrechtlich allerdings nur dann legitim, wenn er an anderen Stelle eingeschränkt wird. Die Entziehung der Freiheit einer Person wäre nicht zur Abwehr jeder Gefahr für die öffentliche Sicherheit, also jedes Verstoßes gegen die objektive Rechtsordnung zu rechtfertigen, und auch nicht zur Verhinderung jeder Straftat. Vielmehr ist ein derart schwerer Grundrechtseingriff nur bei Gefahren für hochwertige Rechtsgüter verfassungsrechtlich legitim. Deswegen ist der Gewahrsamstatbestand auf Gefahren für Rechtsgüter beschränkt, die nach der Rechtsprechung des BVerfG zu den besonders wichtigen Rechtsgüter zu zählen sind, nämlich Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person (etwa: BVerfG, Urt. v. 16. Feb. 2023, 1 BvR 1547/19 = BVerfGE 165, 363 Rn. 105 m. w. N.).

**4.** Weitere Inhalte der Novelle sind neben der aufgezeigten Änderung in Bezug auf die Gewahrsamstatbestände folgende Maßnahmen:

- die Anordnungskompetenz wird klar der Polizei zugeordnet; Ordnungsbehörden erhalten eine kurzfristige Festhaltebefugnis;
- der richterlich angeordnete Gewahrsam wird zeitlich auf eine Höchstdauer begrenzt;

- für den Polizeigewahrsam relevante, an verschiedenen Standorten normierte Regelungen (insbesondere die Benachrichtigung von Vertrauenspersonen und der Richtervorbehalt) werden zusammengeführt;
- die Vorschriften über die Behandlung festgehaltener Personen werden insgesamt weiterentwickelt und modernisiert;
- das Verfahrensrecht wird geschlossen normiert, einschließlich einer Bestellung eines rechtsanwaltlichen Vertreters von Amts wegen in bestimmten Fällen und zur gerichtlichen Überprüfung von Ingewahrsamnahmen.

## V. Weiterentwicklung der elektronischen Aufenthaltsüberwachung

Im Jahr 2021 wurde durch das Gesetz zur Änderung polizei- und ordnungsrechtlicher Vorschriften im Landesverwaltungsgesetz (GVOBl. Schl.-H. S. 222) mit § 201b LVwG erstmals eine Befugnis zur elektronischen Aufenthaltsüberwachung im LVwG geschaffen. Gemäß § 201b LVwG kann die elektronische Aufenthaltsüberwachung angeordnet werden, wenn Tatsachen die Annahme rechtfertigen, dass die überwachte Person eine terroristische respektive eine schwere staatsgefährdende Straftat begehen könnte. Das Einsatzfeld wurde durch die Schaffung der Vorschrift des § 201c LVwG erweitert, die im Jahr 2025 durch das Gesetz zum besseren Schutz von Opfern häuslicher Gewalt und bei Nachstellungen durch den Einsatz der elektronischen Aufenthaltsüberwachung und weitere Änderungen des Landesverwaltungsgesetzes (GVOBl. Schl.-H. Nr. 2025/51) eingeführt wurde. Nach Maßgabe von § 201c LVwG kann die elektronische Aufenthaltsüberwachung als Schutzinstrument in Fällen von häuslicher Gewalt und in gleichgelagerten Stalking-Fällen – und damit zum Schutz wichtiger (individueller) Rechtsgüter in spezifischen Fallkonstellationen – eingesetzt werden.

**1.** Diese Befugnisse zur elektronischen Aufenthaltsüberwachung in § 201b und § 201c LVwG werden neu geordnet und in Teilen neu gestaltet:

- § 201b LVwG-Entwurf übernimmt künftig die in § 201c LVwG ausgeprägte Schutzrichtung der elektronischen Aufenthaltsüberwachung mit Blick auf wichtige Rechtsgüter, jedoch wird der Anwendungsbereich insofern erweitert, als die elektronische Aufenthaltsüberwachung nicht bloß zum Schutz bestimmter gefährdeter Personen angeordnet werden kann. Dadurch ergibt sich die Möglichkeit, die Maßnahme auch dann anzuwenden, wenn der Kreis der gefährdeten Personen nicht individuell, sondern nur anhand bestimmter Kriterien oder Gruppenzugehörigkeiten bestimmbar ist.

- § 201c LVwG-Entwurf greift die bisherige Schutzrichtung des § 201b LVwG auf, also die Abwehr terroristischer Gefahren. Die Neufassung setzt insbesondere Vorgaben des BVerfG aus seiner Entscheidung vom 9. Dezember 2022 zum Sicherheits- und Ordnungsgesetz des Landes Mecklenburg-Vorpommern (1 BvR 1345/21 = BVerfGE 165, 1 Rn. 90 ff., 92) um. Dazu wird der Begriff der „terroristischen Straftat“ eingeführt.

Daneben wird das Anordnungsverfahren in einem selbstständigen neuen § 201d LVwG-Entwurf näher ausgestaltet.
Die Aufteilung der Regelungsbereiche auf zwei Befugnisnormen wird damit aufrechterhalten. Die klare Abschichtung verdeutlicht rechtspolitisch die Heterogenität der Einsatzfelder. Ebenfalls rechtspolitischen Überlegung entspricht es, die Reihenfolge der Befugnisnormen gewissermaßen umzukehren und den Regelungsbereich mit der deutlich höheren praktischen Relevanz, nämlich den Schutz von Individualrechtsgütern insbesondere im Bereich häuslicher Gewalt und in Stalking-Fällen, der „Leit-Vorschrift“ in § 201b LVwG-Entwurf zuzuordnen. Hierdurch wird auch der systematische Zusammenhang zwischen den polizeirechtlichen Maßnahmen zum Schutz bei häuslicher Gewalt gemäß § 201a LVwG und der elektronischer Aufenthaltsüberwachung gemäß § 201b LVwG-Entwurf als Mittel zur Unterstützung und Absicherung dieser Maßnahmen herausgestellt.

**2.** Die elektronische Aufenthaltsüberwachung greift in durchaus erheblicher Weise in Grundrechte ein. Jedoch ist der rechtliche Bezugsrahmen im Verhältnis zum Gewahrsam ein anderer. Trotz der erheblichen Grundrechtsrelevanz stellt die Maßnahme daher ein gegenüber einer Freiheitsentziehung milderes Mittel dar.
Maßgeblich betroffen ist das Recht auf informationelle Selbstbestimmung als Bestandteil des allgemeinen Persönlichkeitsrechts gemäß Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG. In Bezug auf die elektronische Aufenthaltsüberwachung im Bereich der Führungsaufsicht – in dem das Überwachungsinstrument bereits seit 2010 (eingeführt durch das Gesetz zur Neuordnung des Rechts der Sicherungsverwahrung und zu begleitenden Regelungen vom 22. Dezember 2010, BGBl. S. 2300) eingesetzt werden kann – erachtet das BVerfG den Eingriff für verfassungsrechtlich gerechtfertigt (BVerfG, Beschl. v. 1. Dez. 2020, 2 BvR 916/11 pp. = NJOZ 2021, 1391 Rn. 198-219, 259-281 und 295-311). Dabei stützt es sich darauf, dass die Maßnahme der Abwehr einer hinreichend konkretisierten Gefahr für hochrangige Rechtsgüter – Leben, körperliche Unversehrtheit, Freiheit des Einzelnen und sexuelle Selbstbestimmung – verfassungsrechtlich legitim ist (BVerfG a. a. O. Rn. 252, 259-281 und 295-311; vergleiche zur hinreichend konkretisierten Gefahr: Rn. 205, 280). Auch erkennt das BVerfG weder eine Verletzung des Kernbereichs privater Lebensgestaltung noch einen Verstoß gegen das Verbot der „Rundumüberwachung“ (BVerfG a. a. O. Rn. 246-251).
Die einschlägigen Argumente des BVerfG sind auf die polizeirechtliche Einzelmaßnahme übertragbar. Wegen der Einzelheiten ist auf die Begründung des oben genannten Gesetzes zum besseren Schutz von Opfern häuslicher Gewalt und bei Nachstellungen durch den Einsatz der elektronischen Aufenthaltsüberwachung und weitere Änderungen des Landesverwaltungsgesetzes (LT-Drucksache 20/2746) zu verweisen (a. a. O. dort: Seite 18 bis 24).

## B. Einzelbegründung:

## I. Zu Artikel 1 (Änderung des Landesverwaltungsgesetzes)

### 1. Zu Nummer 1 (Inhaltsübersicht):

Die Inhaltsübersicht ist wegen der Änderung der Überschriften von § 184 LVwG, § 201b, § 201c LVwG und § 205 LVwG sowie der Einführung der Vorschriften gemäß §§ 184b, 184c, 188c, 188d, 195b, 195c, 201d und 205a LVwG-Entwurf anzupassen.

### 2. Zu Nummer 2 (Änderung von § 181 Absatz 5 LVwG):

Durch diesen Gesetzentwurf erfährt das Verfahren zur Herbeiführung der richterlichen Entscheidung über die Zulässigkeit und Fortdauer der Ingewahrsamnahme eine selbständige, geschlossene und in wesentlichen Punkten neu gestaltete Vorschrift in § 205a LVwG. Diese Regelung hat künftig auch für Richtervorbehalt im Fall einer Freiheitsentziehung zum Zwecke der Identitätsfeststellung durch Verweisung Geltung und löst den bisherigen § 181 Absatz 5 LVwG ab.

### 3. Zu Nummer 3 (Änderung von § 184 LVwG):

Die Befugnis zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen im öffentlichen Raum wird redaktionell überarbeitet und in einzelnen Punkten erweitert.

#### a. Zu § 184 Absatz 1 LVwG-Entwurf:

§ 184 Absatz 1 LVwG wird redaktionell angepasst.

#### b. Zu § 184 Absatz 2 LVwG-Entwurf:

§ 184 Absatz 2 Satz 1 LVwG-Entwurf führt den bisherigen Regelungsgehalt des § 184 Absatz 2 Satz 1 LVwG fort.
Die Ausgliederung in einen eigenen Absatz dient der klareren Abschichtung von Bildübertragungen einerseits und Bildaufnahmen und -aufzeichnungen andererseits. Die Bildübertragung im Sinne des Satzes 1 berechtigt nur zur Anfertigung von Übersichtsaufnahmen ohne Personenbezug (Martens in PdK SH A-15, LVwG § 184 Anm. 2.3.1).
§ 184 Absatz 2 Satz 2 LVwG-Entwurf definiert den auch bisher in § 184 LVwG verwendeten Begriff des allgemein zugänglichen Raumes näher und schafft eine Regelung in Bezug auf befriedetes Besitztum, jeweils in Übereinstimmung und zur Harmonisierung mit § 184a Absatz 1 Satz 1 LVwG, also der Vorschrift über den Einsatz körpernah getragener Aufnahmegeräte (sogenannte Body-Cams).

### c. Zu § 184 Absatz 3 LVwG-Entwurf:

Der neue § 184 Absatz 3 LVwG-Entwurf übernimmt einerseits den Regelungsgehalt der bisher in § 184 Absatz 2 Satz 2 LVwG enthaltenen Befugnis zur Anfertigung offener Bild- und Tonaufnahmen oder -aufzeichnungen von Personen an allgemein zugänglichen Orten, erweitert diese Befugnis jedoch andererseits in zwei Punkten. Den Kern der bisher in § 184 Absatz 2 Satz 2 LVwG enthaltenen Befugnis übernimmt § 184 Absatz 3 Satz 1 Nummer 2 LVwG-Entwurf. Die Erweiterungen beziehen sich auf § 184 Absatz 3 Satz 1 Nummer 1 und 3 LVwG-Entwurf:

Zum einen wird mit § 184 Absatz 3 Satz 1 Nummer 1 LVwG-Entwurf die Möglichkeit eröffnet, offene Bild- und Tonaufnahmen oder -aufzeichnungen von Personen an allgemein zugänglichen Orten im Einzelfall zur Abwehr einer Gefahr für die öffentliche Sicherheit zu erstellen. Bild- und Tonaufnahmen und -aufzeichnungen nach Nummer 2 und Nummer 3 sind nur an Orten gestattet, die auf Grundlage von Lageerkenntnissen oder polizeilicher Erfahrung als besonders gefährlich eingestuft sind. Liegen solche Erkenntnisse (noch) nicht vor, könnten Bild- und Tonaufnahmen und -aufzeichnungen auch dann nicht angefertigt werden, wenn dies zur Abwehr der Gefahr im Einzelfall erforderlich ist, zum Beispiel bei konkreten Hinweisen auf einen Terroranschlag auf einem bislang nicht als Kriminalitätsschwerpunkt kategorisierten Stadtplatz. Durch § 184 Absatz 3 Satz 1 Nummer 1 LVwG-Entwurf erhält die Polizei mithin die Möglichkeit, mit dem Mittel der Videoüberwachung flexibel auf Gefahrenlagen zu reagieren.

Zum anderen eröffnet § 184 Absatz 3 Satz 1 Nummer 3 LVwG-Entwurf der Polizei die Möglichkeit, Bild- und Tonaufnahmen und -aufzeichnungen an sogenannten gefährlichen und gefährdeten Orten vorzunehmen. Erforderlich ist, dass jeweils die Voraussetzungen des § 181 Absatz 1 bis 3 LVwG für die Einstufung dieser Orte vorliegen; das gilt insbesondere für die in diesen Vorschriften im Einzelnen geforderten Gefahrenprognosen, deren Vorliegen zudem schriftlich zu dokumentieren ist. Sogenannte gefährliche Orte im Sinne von § 181 Absatz 1 Nummer 1 LVwG werden häufig von den Bürgerinnen und Bürgern als „Angsträume“ wahrgenommen. Durch Videoüberwachung kann hier eine positive Wirkung auf die Sicherheitslage erreicht werden. Im Bereich des Bahnhofs Elmshorn und in dessen Umfeld nahm die Anzahl von Gewalttaten, Diebstählen und Sachbeschädigungen mit Einführung einer auf die geltende Fassung des § 184 Absatz 2 Satz 2 LVwG gestützten Videoüberwachung signifikant ab. Zugleich ermöglicht § 184 Absatz 3 Nummer 3 LVwG-Entwurf besonders schützenswerte Objekte, zum Beispiel Versorgungs- oder Verkehrseinrichtungen, durch eine Videoüberwachung (ergänzend) zu sichern.

### d. Zu § 184 Absatz 4 LVwG-Entwurf:

§ 184 Absatz 4 LVwG-Entwurf übernimmt den Regelungsgehalt des bisherigen § 184 Absatz 3 Satz 1 LVwG. Die Beschränkung auf öffentlich zugängliche Orte dient der Klarstellung. Auch die geltende Befugnisnorm des § 184 Absatz 3 LVwG gestattet keine Aufnahmen und Aufzeichnungen in Wohnungen oder an anderen Orten, die dem Schutzbereich

des Artikels 13 GG unterfallen (Büttner/Schade/Scholze/Susel, Polizei- und Ordnungsrecht in Schleswig-Holstein, S. 163).
Die in § 184 Absatz 3 Satz 2 und 3 LVwG enthaltenen Regelungen zur Speicherung und zweckändernden Weiterverarbeitung werden in § 184 Absatz 6 LVwG-Entwurf überführt.

**e. Zu § 184 Absatz 5 LVwG-Entwurf:**

§ 184 Absatz 5 LVwG-Entwurf führt eine Rechtsgrundlage für den Einsatz automatisierter Anwendungen zur Mustererkennung neu ein.

Akute Bedrohungssituationen können bei ausschließlichem Einsatz menschlichen Personals im Moment ihres Entstehens nur eingeschränkt erfasst und bewertet werden. Studien weisen darauf hin, dass eine manuelle Auswertung von Videodaten häufig nicht effektiv ist, da die Aufmerksamkeit bei der Überwachung von Monitoren bereits nach kurzer Zeit signifikant abnimmt. Automatisierte Videoüberwachungssysteme, die Situationen oder Personen mittels Algorithmen bewerten, leisten hier wertvolle Abhilfe und tragen zugleich dazu bei, sogenanntes „Social Sorting“ zu vermeiden. Es wird unterbunden, dass Menschen ohne sachlichen Grund aufgrund ihrer Ethnie oder Herkunft das Attribut „gefährlich“ zugewiesen wird. Eine potenziell stigmatisierende Wirkung der Videoüberwachung wird reduziert. Das Ziel der Mustererkennung ist eine vorurteilsfreie Situationseinschätzung, die durch eine automatisierte Bildauswertung als Grundlage für die polizeiliche Lagebeurteilung dient. Die Darstellung der überwachten Personen erfolgt dabei anonymisiert oder pseudonymisiert. Für die Mustererkennung werden – über die Bildaufnahmen und -aufzeichnungen hinaus – keine weiteren personenbezogenen oder biometrischen Daten erhoben und verarbeitet.

Ein abgestuftes Vorgehen ermöglicht die Reduzierung des verarbeiteten Datenumfangs. Zunächst werden auf technischem Wege Muster erkannt, die auf bestimmte Gefahren hinweisen, deren Bestehen menschlich bestätigt werden muss, bevor gegebenenfalls erforderliche Maßnahmen zielgerichtet gegen Personen, von denen eine Gefahr ausgeht, ergriffen werden dürfen. Die Mustererkennung bezweckt in gefahrgeneigten Bereichen die automatisierte Identifikation interventionsbedürftiger Situationen durch die Klassifizierung visueller Muster. Dazu werden die Bewegungen der überwachten Personen analysiert und auf Abweichungen von vordefinierten Mustern hin ausgewertet.
Das Markieren einer Person nach Satz 3 dient der gezielten Überwachung von Personen, von denen Gefahren ausgehen, und ist nur erforderlich, wenn die beobachtete Person Adressat weiterer Maßnahmen werden soll. Es erfolgt keine automatisierte Identifizierung der markierten Person. Die Verarbeitung biometrischer Daten ist auf das technisch erforderliche Maß zu beschränken. Es sollen vorrangig nicht körperliche Merkmale – etwa auffällige Kleidungsstücke, Schuhe oder Ähnliches – zur Kennzeichnung herangezogen werden.
Die Markierung einer Person zur Nachverfolgung sowie die Veranlassung oder Anordnung weitergehender Maßnahmen nach anderen Vorschriften obliegen ausschließlich dem Ermessen hinreichend qualifizierten Beschäftigten der Polizei, wodurch das Verbot automatisierter Einzelentscheidungen gemäß § 30 des Schleswig-Holsteinischen Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz – LDSG) gewahrt wird.

Eine automatisierte biometrische Fernidentifizierung (unabhängig davon, ob sie in Echtzeit oder nachträglich erfolgt) ist auf Grundlage von § 184 Absatz 5 LVwG-Entwurf nicht zulässig. Dies ergibt sich bereits daraus, dass § 24 Absatz 3 LDSG ausdrücklich regelt, dass die Verarbeitung biometrischer Daten in einer Rechtsvorschrift geregelt sein muss. Zur Klarstellung ordnet § 184 Absatz 5 Satz 4 Halbsatz 2 LVwG-Entwurf dasselbe explizit an.

### f. Zu § 184 Absatz 6 LVwG-Entwurf:

Die Speicherfristen und Regelungen über eine zweckändernde Weiterverarbeitung für alle Aufnahmen und Aufzeichnungen nach § 184 LVwG-Entwurf werden in § 184 Absatz 6 LVwG-Entwurf zusammengeführt.
Die de lege lata sehr kurze Frist von drei Tagen für die Speicherung von Bildaufnahmen und Bild- und Tonaufzeichnungen zum Schutz von Polizeibeamtinnen und Polizeibeamten wird auf bis zu einem Monat erweitert. Damit wird eine Annäherung an die – an demselben Zweck ausgerichteten – Vorschriften zum Einsatz körpernah getragener Aufnahmegeräte (sogenannte Body-Cams) gemäß § 184a Absatz 6 LVwG erreicht.
Die Speicherbefugnis zur Straftatenverhütung gemäß § 184 Absatz 4 Satz 2 Alternative 2 LVwG („Tatsachen dafür sprechen, dass die Person künftig vergleichbare Straftaten oder Straftaten im Sinne des § 179 Absatz 2 [LVwG] begehen wird“) wird in § 184 Absatz 6 Nummer 2 LVwG-Entwurf übernommen und um eine an § 196 LVwG orientierte Formulierung ergänzt, welche nun vorsieht, dass die Kenntnis der Aufzeichnungen für die speichernde Stelle zur Aufgabenerfüllung erforderlich sein muss.
Als weiterer Grund für eine zweckändernde Weiterverarbeitung wird die Überprüfung der Rechtsmäßigkeit polizeilicher Maßnahmen eingeführt. Vorbild ist auch hier § 184a Absatz 6 LVwG.

### g. Zu § 184 Absatz 7 LVwG-Entwurf:

§ 184 Absatz 7 Satz 1 und 2 LVwG-Entwurf übernimmt den Regelungsgehalt von § 184 Absatz 1 Satz 4 und Absatz 5 LVwG.
Allerdings wird die bisher in § 184 Absatz 5 LVwG enthaltene Regelung, nach der auf die Kenntlichmachung von Videoaufzeichnungen verzichtet werden kann, soweit nicht die Maßnahme im Einzelfall offensichtlich ist, nicht ins neue Recht überführt. Die Einschränkung der Hinweispflicht dürfte bereits aufgrund des wertungsoffenen Begriff „offensichtlich“ nur geringe praktische Bedeutung gehabt haben.
Ergänzt wird außerdem die Pflicht, auf die Verwendung einer automatisierten Anwendung zur Mustererkennung gemäß § 184 Absatz 5 LVwG-Entwurf gesondert hinzuweisen.
Die bisher in § 184 Absatz 4 Satz 5 LVwG geregelte Benachrichtigungspflicht respektive das Absehen von einer Benachrichtigung wird nicht fortgeführt. Es handelt sich bei den Maßnahmen nach § 184 Absätze 1 bis 4 LVwG-Entwurf um offene Datenerhebungen, auf die Betroffene hingewiesen werden. Dadurch sind die erforderliche Transparenz und die Möglichkeit, Rechtsschutz in Anspruch zu nehmen, gewährleistet.

## 4. Zu Nummer 4 (Einführung von §§ 184b, 184c LVwG-Entwurf):

**a. Zu § 184b LVwG-Entwurf**

Mit § 184b LVwG-Entwurf wird eine Rechtsgrundlage für eine sogenannte biometrische Echtzeit-Fernidentifizierung eingeführt (vergleiche zum Begriff: Allgemeiner Teil Punkt II.).

**b. Zu § 184b Absatz 1 LVwG-Entwurf:**

Die biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen kombiniert die klassische Videoüberwachung mit einer automatisierten Datenverarbeitung. Dazu werden aus Bild- und Tonaufnahmen oder -aufzeichnungen von Personen, die aus Maßnahmen nach § 184 Absatz 1 oder 3 LVwG-Entwurf erlangt werden, biometrische Daten gewonnen und mit den biometrischen Daten einer Person abgeglichen, nach der gesucht wird.

Die biometrische Echtzeit-Fernidentifizierung knüpft zwar an Maßnahmen zur Videoüberwachung nach § 184 Absatz 1 und 3 LVwG-Entwurf an. Gleichwohl handelt es sich bei der Datenerhebung bei öffentlichen Veranstaltung und Ansammlungen sowie auf öffentlichen Flächen einerseits und der biometrischen Echtzeit-Fernidentifizierung andererseits um eigenständige Datenverarbeitungsbefugnisse. Das heißt, erst wenn die hohe Eingriffsschwelle des § 184b LVwG-Entwurf erreicht und besonders wichtige Rechtsgüter zu schützen sind, dürfen die Videoaufzeichnungen für eine Echtzeit-Fernidentifizierung nutzbar gemacht werden. Bereits dadurch wird deutlich, dass die biometrische Echtzeit-Fernidentifizierung nicht dazu eingesetzt werden kann, im Allgemeinen Informationen über Personen zu sammeln, die auf Bild- und Tonaufnahmen oder -aufzeichnungen erkennbar sind. Tatbestandlich sichert außerdem die Voraussetzung, nach der eine biometrische Echtzeit-Fernidentifizierung nur zur „Ergänzung eines vorhandenen Sachverhalts“ durchgeführt werden darf, dass die Maßnahme ausschließlich in Bezug auf einen konkreten gefahrenabwehrrechtlich relevanten Sachverhalt durchgeführt wird. Es ist also ausgeschlossen, dass sie zum Selbstzweck oder anlasslose erfolgt.

Zielrichtung der Maßnahme ist die Identität zwischen einer bestimmten Person und einer auf Bild- und Tonaufnahmen oder -aufzeichnungen erkennbaren Person anhand biometrischer Merkmale zu bestätigen. Dazu dürfen aus verfügbaren Daten – dem Datensatz einer bestimmten Person und den Daten der Personen, die auf den Videoaufzeichnungen erkennbar sind – biometrische Daten gewonnen werden. Der Begriff der „biometrischen Daten“ entspricht hier der Legaldefinition in § 21 Nummer 12 LDSG beziehungsweise der Begriffsbestimmung in Artikel 3 Nummer 34 der KI-Verordnung. Es handelt sich um die mit speziellen technischen Verfahren gewonnenen personenbezogenen Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die eine eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen. „Erkennbar“ ist eine Person auf den Bild- und Tonaufnahmen oder -aufzeichnungen, wenn biometrisch auswertbare Daten (insbesondere ihres Gesichts oder ihrer Stimme) auf den Aufnahmen und Aufzeichnungen feststellbar sind.
Die Erfassung der biometrischen Daten, der Abgleich und die Identifizierung dürfen im Rahmen von § 184b LVwG-Entwurf „in Echtzeit“, das heißt nahezu zeitgleich beziehungsweise ohne erhebliche Verzögerung erfolgen (vergleiche die Definition für ein biometrisches Echtzeit-Fernidentifizierungssystem gemäß Artikel 3 Nummer 42 der KI-

Verordnung). Darin unterscheidet sich der biometrische Abgleich gemäß § 184b LVwG-Entwurf von der in § 195b LVwG-Entwurf normierten Maßnahme (nachträgliche Fernidentifizierung), bei der in einem gesonderten Erhebungsschritt aus dem Internet gewonnene Daten verwendet werden.

Die Voraussetzungen für die Zulässigkeit der biometrischen Echtzeit-Fernidentifizierung speisen sich aus zwei Quellen:

- Da der Einsatz KI-getriebener biometrischer Echtzeit-Fernidentifizierungssysteme eine von der KI-Verordnung grundsätzlich verbotene und nur unter engen Voraussetzungen erlaubte Praktik im Sinne dieses Regelungswerks darstellt, ist der Regelungsrahmen zu einen durch das europäische Recht als spezifisches Regelungsregime für den Einsatz von KI-Systemen vorgeprägt.
- Die KI-Verordnung bildet jedoch nur einen Aspekt der für die Normierung des Einsatz von biometrischen Echtzeit-Fernidentifizierungssystemen maßgeblichen Leitlinien ab. Zum anderen ergeben sich aus nationalen verfassungsrechtlichen Vorgaben Grenzen für die Verwendung solcher Systeme.

Den Einsatz KI-getriebener biometrischer Echtzeit-Fernidentifizierungssysteme zu Zwecken der Strafverfolgung lässt die KI-Verordnung nur in engen – in Artikel 5 Unterabsatz 1 Buchstabe h sowie Artikel 5 Absätze 2 bis 7 der KI-Verordnung beschriebenen – Grenzen zu. Unter Strafverfolgung im Sinne der KI-Verordnung ist auch eine Tätigkeit zu verstehen, die auf die Verhütung von Straftaten zielt, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (vergleiche Artikel 3 Nummer 46 der KI-Verordnung). Letztlich kommt es auf diese Einordnung nicht entscheidend an, da das Verbot des Artikel 5 Unterabsatz 1 Buchstabe h der KI-Verordnung (einschließlich der Ausnahmetatbestände) gemäß Artikel 5 Unterabsatz 2 der KI-Verordnung auch für die Verarbeitung biometrischer Daten zu anderen Zwecken als der Strafverfolgung Anwendung findet.

Die KI-Verordnung gibt den Rahmen für eine im nationalen Recht zu schaffende Rechtsgrundlage zum Einsatz eines KI-getriebenen biometrischen Echtzeit-Fernidentifizierungssystems vor (vergleiche Artikel 5 Absatz 5 Satz 1 und 3 der KI-Verordnung). Eine solche Rechtsgrundlage enthält § 184b Absatz 1 LVwG-Entwurf. Die Befugnisnorm kann allerdings die detailreichen Einsatzvoraussetzungen, Genehmigungserfordernisse und weiteren Rahmenbedingungen aufgrund des europarechtlichen Normwiederholungsverbots (vergleiche EuGH, Urt. v. 10. Oktober 1973, 34/73 = BeckRS 2004, 70873 Rn. 9 bis 11; Streinz/W. Schroeder, 3. Aufl. 2018, AEUV Art. 288 Rn. 43) nicht selbst regeln, sondern lediglich auf das unmittelbar geltende Recht der KI-Verordnung verweisen. Im Wesentlichen setzt der Normentwurf folgende Vorgaben um:

- Von den Zielen der KI-Verordnung, die den Einsatz von Systemen zur biometrischen Echtzeit-Fernidentifizierung nach Artikel 5 Unterabsatz 1 Buchstabe h legitimieren können, greift § 184b LVwG-Entwurf folgende Verwendungszwecke auf:
  - § 184b Absatz 1 Satz 3 Nummer 1: die gezielte Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie die Suche nach vermissten Personen;

  - § 184b Absatz 1 Satz 3 Nummer 2: Abwehr einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen;
  - § 184b Absatz 1 Satz 3 Nummer 3: die Gefahr eines Terroranschlags;

- § 184b Absatz 1 Satz 1 bildet das in Artikel 5 Absatz 2 der KI-Verordnung vorgegebene Einsatzziel ab, nämlich die „Bestätigung der Identität der speziell betroffenen Person“.

- § 184b Absatz 1 Satz 4 weist auf die nach Artikel 5 Absatz 2 Satz 1 Buchstabe a und b der KI-Verordnung zu beachtenden Abwägungsgesichtspunkte hin sowie die weiteren Voraussetzungen für den Einsatz solche Systeme, nämlich:
  - die Einhaltung der – im nationalen Recht umzusetzenden – „notwendigen und verhältnismäßigen Schutzvorkehrungen und Bedingungen für die Verwendung […], insbesondere in Bezug auf die zeitlichen, geografischen und personenbezogenen Beschränkungen“ (vergleiche dazu § 184b Absatz 2 LVwG-Entwurf) und
  - eine Folgenabschätzung im Hinblick auf die Grundrechte gemäß Artikel 27 der KI-Verordnung und die Registrierung des eingesetzten Systems gemäß Artikel 49 der KI-Verordnung.

Die Vorgaben der KI-Verordnung gelten im Grundsatz nur insoweit ein KI-System im Sinne dieser Verordnung (vergleiche Artikel 3 Nummer 1 der KI-Verordnung) eingesetzt wird. Um jedoch im Einzelfall schwierige Abgrenzungs- und Subsumtionsfragen zu vermeiden, sind gemäß § 184b Absatz 1 Satz 5 LVwG-Entwurf die Voraussetzungen des § 184b LVwG-Entwurf für jede biometrische Echtzeit-Fernidentifizierung zu beachten, das heißt unabhängig davon, ob die eingesetzte Software als ein KI-System im Sinne von Artikel 3 Nummer 1 der KI-Verordnung einzustufen ist.

Die KI-Verordnung schafft ein spezifisches Regelungsregime für den Einsatz von KI-Systemen. Sie bildet jedoch nur einen Aspekt des für den Einsatz von biometrischen Echtzeit-Fernidentifizierungssystemen maßgeblichen Rechtsrahmens. Daneben sind verfassungsrechtlichen Grenzen zu beachten:
Die Maßnahme ist eingriffsintensiv. Da die biometrischen Daten eines Menschen nahezu unveränderlich sind und „dem offenen Zeigen des eigenen Gesichts“ in einem freiheitlichen Gesellschaftsverständnis eine besondere Bedeutung zukommt, weist die zustimmungsfreie Fernidentifizierung von Menschen zwar ein hohes Potenzial für die polizeiliche Aufgabenerfüllung auf, ist gleichzeitig aber auch mit einer besonderen grundrechtlichen Gefährdungslage verbunden.
Nach der Rechtsprechung des BVerfG muss eine Rechtsgrundlage, welche die Gewinnung einer große Datenmenge potenziell unbeteiligter Personen zum Zweck eines Abgleichs gestattet, der Abwehr konkreter Gefahren für hochrangige Rechtsgüter dienen (BVerfG, Beschl. 4. Apr. 2006, 1 BvR 518/03 = BVerfGE 115, 320, 360 ff.; BVerfG, Urt. 20. Apr. 2016, 1 BvR 966/09 pp. = BVerfGE 141, 202 Rn. 207). Eine hinreichend konkretisierte Gefahr würde nicht genügen (instruktiv BVerfG, Beschl. v. 9. Dez. 2022, 1 BvR 1345/21 = BVerfG E 165, 1 Rn. 185 ff.). Die zur Rasterfahndung formulierten Grundsätze gelten für eine Fernidentifizierung entsprechend, die sich Bild- und Tonaufnahmen oder

-aufzeichnungen von Personen auf allgemein zugänglichen Flächen und in öffentlich zugänglichen Räumen als Datenquelle bedient. Der Umstand, dass die aufgenommenen Personen, deren Daten verwendet werden, sich in der Öffentlichkeit bewegt haben, führt zu keiner anderen Bewertung, da dieser Umstand nichts an der Tatsache ändert, dass auch bei der Gewinnung solcher Daten das die Rasterfahndung prägende Merkmal erfüllt ist. Dies besteht darin, dass die einbezogenen Daten keinen Bezug zur Gefahrenlage haben, die Maßnahme für die Betroffenen mithin anlasslos ist (vergleiche BVerfG a. a. O.).
Die biometrischen Echtzeit-Fernidentifizierung nach § 184b LVwG-Entwurf ist daher nur zulässig zur Abwehr einer konkreten Gefahr für Rechtsgüter, die nach der Rechtsprechung des BVerfG zu den besonders wichtigen Rechtsgütern zu zählen sind (zu diesem Begriff: BVerfG, Urt. v. 16. Feb. 2023, 1 BvR 1547/19 = BVerfGE 165, 363 Rn. 105 m. w. N.). Hieraus resultieren die entsprechende Ergänzungen der europarechtlichen Vorgaben in § 184b Absatz 1 Satz 3 Nummer 1 und 3 LVwG-Entwurf. In Bezug auf § 184b Absatz 1 Satz 3 Nummer 2 LVwG-Entwurf entspricht die Vorgabe der KI-Verordnung den verfassungsrechtlichen Anforderungen. In diesem Fall ist die biometrische Echtzeit-Fernidentifizierung zur Abwehr „einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen“ gestattet.

Aus der Regelung des § 24 LDSG über die Verarbeitung besonderer Kategorien personenbezogener Daten ergeben sich keine weiteren Restriktionen. Angesichts der hohen Schwelle des § 184b Absatz 1 Satz 3 LVwG-Entwurf wird die Datenverarbeitung regelmäßig der Wahrung lebenswichtiger Interessen der von der Datenverarbeitung betroffenen oder einer anderen natürlichen Person im Sinne von § 24 Absatz 1 Nummer 2 LDSG dienen. Aufgrund der europarechtlichen Vorgaben des Artikel 5 Unterabsatz 1 Buchstabe h der KI-Verordnung darf der Abgleich allerdings nur durchgeführt werden, wenn dies unbedingt erforderlich ist. In Abgrenzung zu einer zwingenden Erforderlichkeit des § 24 Absatz 1 Nummer 1 LDSG beziehungsweise Unverzichtbarkeit impliziert diese lediglich eine strenge Verhältnismäßigkeitsprüfung, verbunden mit einer intensiven Suche nach milderen Maßnahmen.

### c. Zu § 184b Absatz 2 LVwG-Entwurf:

Artikel 5 Absatz 2 Satz 2 der KI-Verordnung fordert, dass die nationalen Ermächtigungen, mit denen der Einsatz von Systemen zur biometrischen Echtzeit-Fernidentifizierung gemäß Artikel 5 Absatz 5 Satz 1 bis 3 der KI-Verordnung vorgesehen werden, Beschränkungen unter „zeitlichen, geografischen und personenbezogenen“ Gesichtspunkten enthalten. Dies setzt § 184b Absatz 2 LVwG-Entwurf um.
Gemäß § 184b Absatz 2 Satz 1 LVwG-Entwurf ist die biometrische Echtzeit-Fernidentifizierung im Einzelfall auf das zeitlich und örtlich unbedingt erforderliche Maß zu begrenzen. Hinzukommt, dass eine Maßnahme gemäß § 184b Absatz 3 Satz 2 LVwG-Entwurf jeweils nur für höchstens 7 Tage angeordnet werden darf.
Darüber hinaus normiert § 184b Absatz 2 Satz 2 LVwG-Entwurf eine personenbezogene Beschränkung. Die biometrische Echtzeit-Fernidentifizierung darf nur zu dem Ziel durchgeführt werden, auf den Bild- und Tonaufnahmen oder -aufzeichnungen entweder das Opfer einer Entführung, des Menschenhandels oder der sexueller Ausbeutung oder eine

vermisste Person zu identifizieren (§ 184b Absatz 2 Satz 2 Nummer 1 LVwG-Entwurf) oder die Person zu identifizieren, die für die Gefahrenlage verantwortlich ist (§ 184b Absatz 2 Satz 2 Nummer 2 LVwG-Entwurf). Das heißt, der biometrische Abgleich darf nur die biometrischen Daten dieser Person zum Ausgangspunkt haben.

**e. Zu § 184b Absatz 3 und 4 LVwG-Entwurf:**

Gemäß Artikel 5 Absatz 5 Satz 2 der KI-Verordnung sind die Vorschriften für die Beantragung, Erteilung und Ausübung der nach Artikel 5 Absatz 3 der KI-Verordnung erforderlichen Genehmigung für den Einsatz eines KI-getriebenen biometrischen Echtzeit-Fernidentifizierungssystems im nationalen Recht festzulegen. § 184b Absatz 3 und 4 LVwG-Entwurf setzten dies im Einzelnen um.
Für eine biometrische Echtzeit-Fernidentifizierung bedarf es einer richterlichen Anordnung, die, wie die Rasterfahndung (§ 195a Absatz 2 LVwG), die Antragsstellung durch die Amts- oder Behördenleitung oder eine hierzu besonders beauftragte Person des Polizeivollzugsdienstes voraussetzt. Es besteht jedoch die Möglichkeit mit der biometrischen Echtzeit-Fernidentifizierung ohne vorherige richterliche Genehmigung zu beginnen; jedoch ist in diesem Fall eine nachträgliche richterliche Genehmigung binnen 24 Stunden zu beantragen.
Für die gerichtliche Zuständigkeit und das gerichtliche Verfahren gelten die allgemeinen Regeln des § 186 Absatz 6 LVwG. Die Richterin oder der Richter hat den von Artikel 5 Absatz 3 Unterabsatz 2 Satz 1 und 2 der KI-Verordnung vorgegebenen Prüfungsmaßstab zu beachten und die Entscheidung entsprechend § 186 Absatz 3 Satz 1 und 2 LVwG schriftlich zu begründen.

**g. Zu § 184c LVwG-Entwurf:**

§ 184c LVwG-Entwurf enthält Regelungen für die Durchführung der Echtzeit-Fernidentifizierung nach § 184b LVwG-Entwurf. Sie setzt – im Falle des Einsatzes eines KI-Systems im Sinne der KI-Verordnung – die in Artikel 5 Absatz 5 Satz 2 der KI-Verordnung enthaltene Verpflichtung des nationalen Gesetzgebers um, die erforderlichen Vorschriften über die Ausübung einer Genehmigung, die eine solche Maßnahme gestattet, sowie über Beaufsichtigung und Berichterstattung vorzusehen.

**h. Zu § 184c Absatz 1 LVwG-Entwurf:**

§ 184c Absatz 1 LVwG-Entwurf trifft wichtige Vorkehrungen zum Grundrechtsschutz bei der Durchführung der Echtzeit-Fernidentifizierung nach § 184b LVwG-Entwurf.

Zuvörderst normiert § 184c Absatz 1 Satz 1 LVwG-Entwurf eine strenge Zweckbindung der verarbeiteten biometrischen Daten. Diese bezieht sich nicht nur auf den Zweck der Datenerhebung, also die Abwehr von Gefahren für bestimmte besonders wichtige Rechtsgüter, sondern auch auf den konkreten Sachverhalt, der Anlass für die Durchführung der biometrischen Echtzeit-Fernidentifizierung war. Damit ist sowohl jede zweckkonforme Nutzung nach § 188a Absatz 1 LVwG als auch die zweckändernde Weiterverarbeitung nach § 188a Absatz 2 LVwG ausgeschlossen. Auf diese Weise wird das Entstehen einer (unspezifischen) Datenbank ohne konkreten Fallbezug unterbunden.

Um die Beeinträchtigung Unbeteiligter zu reduzieren, dürfen außerdem allein auf Grundlage des von der Anwendung angebotenen Abgleichergebnisses keine Folgemaßnahmen getroffen werden. Vielmehr bedarf es stets einer menschlichen Prüfung des Abgleichergebnisses. Dies entspricht der Vorgabe aus Artikel 5 Absatz 3 Unterabsatz 2 Satz 3 der KI-Verordnung, dass eine Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, nicht ausschließlich auf der Grundlage der Ausgabe des biometrischen Echtzeit-Fernidentifizierungssystems getroffen werden darf. Artikel 14 Absatz 5 Unterabsatz 1 der KI-Verordnung sieht für Hochrisiko-KI-Systeme vor, dass eine Überprüfung des Identifizierungsvorgangs von zwei entsprechend qualifizierten natürlichen Personen vorzunehmen ist. Zwar kann von dieser Vorgabe gemäß Artikel 14 Absatz 5 Unterabsatz 2 der KI-Verordnung abgewichen werden, die in den Bereichen Strafverfolgung, Migration, Grenzkontrolle oder Asyl verwendet werden. Die Voraussetzung hierfür – dass nämlich die Überprüfung durch zwei Beschäftigte „unverhältnismäßig wäre“ – lässt sich für die herausgehobenen Einsatzszenarien, die § 184b LVwG-Entwurf im Blick hat, nicht begründen.
Die menschliche Prüfung nach § 184c Absatz 1 Satz 2 LVwG-Entwurf stellt zugleich das auslösende Moment für die Befugnis dar, die zum Zwecke des Abgleichs zusammengeführten Daten weiterhin in den polizeilichen Systemen zu speichern. Ergibt die Prüfung, dass auf Grundlage des Abgleichergebnisses weitere Maßnahmen erforderlich sind, dürfen die mit dieser Entscheidung zusammenhängenden Daten nach den allgemeinen Regeln zur Aufgabenerfüllung gespeichert werden. Für alle anderen Daten besteht ein uneingeschränktes Verarbeitungsverbot. Sie sind zu löschen.

### i. Zu § 184c Absatz 2 LVwG-Entwurf:

Die Benachrichtigung dient der Transparenz hoheitlichen Handelns. Sie ist bei verdeckten Maßnahmen Grundvoraussetzung des Rechtsschutzes.

### j. Zu § 184c Absatz 3 LVwG-Entwurf:

§ 184c Absatz 3 LVwG-Entwurf trifft Regelungen zur Transparenz und zur Nachvollziehbarkeit grundrechtsintensiven Handelns.
Zu demselben Zweck wird § 184b LVwG-Entwurf in den Kanon der Vorschriften zur Protokollierung bestimmter eingriffsintensiver Maßnahmen nach § 186c LVwG aufgenommen. § 184c Absatz 3 Satz 2 LVwG-Entwurf normiert darüber hinaus bestimmte spezielle Protokollierungspflichten. Über in § 186c LVwG vorgeschriebene Protokollierung hinaus sind die eingesetzte automatisierte Anwendung zur Datenverarbeitung und die Mitarbeiterin oder der Mitarbeiter zu erfassen, die oder der die Maßnahme durchführt.
Die Aufnahme des § 184b LVwG-Entwurf in § 186c LVwG hat auch zur Folge, dass die oder der Landesbeauftragte für Datenschutz gemäß § 186b Absatz 1 LVwG zu Stichproben-Kontrollen verpflichtet ist und eine Berichtspflicht gegenüber dem Landtag gemäß § 186b Absatz 2 LVwG besteht.
Soweit eine tiefergehende gesetzliche Normierung wegen der besonderen Technizität und der raschen Fortentwicklungsbedürftigkeit von automatisierten Anwendungen zur Datenverarbeitung nicht praktikabel ist, hat das BVerfG dem Gesetzgeber gestattet, die Verwaltung zu ermächtigen, die nähere Regelung organisatorischer und technischer Einzelheiten in einer Verwaltungsvorschrift weiter zu konkretisieren (Urt. v. 16. Feb. 2023,

1 BvR 1547/19 pp. = BVerfGE 165, 363 Rn. 112 ff.). Nach Maßgabe des Gesetzesvorbehalts muss der Gesetzgeber aber die wesentlichen Vorgaben hinreichend bestimmt und normenklar selbst regeln.

**5. Zu Nummer 5 (Änderung von § 186b Absatz 2 LVwG):**

Gemäß § 186b Absatz 2 LVwG unterrichtet die Landesregierung den Landtag jährlich über Anlass, Umfang, Dauer und Ergebnis der nach § 186c LVwG zu protokollierenden eingriffsintensiven Maßnahmen. Von dieser Berichtspflicht wird jedoch der IT-gestützte Abgleich gemäß § 188c Absatz 1 LVwG-Entwurf ausgenommen. Die Eingriffsintensität dieser Maßnahme bleibt deutlich hinter den berichtspflichtigen verdeckten Überwachungsmaßnahmen und ihnen gleichzustellenden Eingriffen zurück.

**6. Zu Nummer 6 (Änderung von § 186c LVwG):**

Die neu eingeführten Befugnisnormen

- Echtzeit-Fernidentifizierung gemäß § 184b LVwG-Entwurf,
- nachträgliche Fernidentifizierung gemäß § 195b LVwG-Entwurf,
- IT-gestützter Abgleich gemäß § 188c Absatz 1 und
- (automatisierte) Datenanalyse gemäß § 188c Absatz 2

werden in den Kanon des § 186c LVwG zur Protokollierung bestimmter eingriffsintensiver Maßnahmen aufgenommen. Zu beachten ist allerdings, dass

- § 184c Absatz 3 Satz 2 LVwG-Entwurf (Echtzeit-Fernidentifizierung)
- § 188d Absatz 4 Satz 2 LVwG-Entwurf (Datenanalyse)
- § 195c Absatz 3 Satz 2 LVwG-Entwurf (nachträgliche Fernidentifizierung)

übereinstimmend jeweils bestimmte weitergehende Protokollierungspflichten normieren. Über die in § 186c LVwG vorgeschriebene Protokollierung hinaus sind die eingesetzte automatisierte Anwendung zur Datenverarbeitung und die Mitarbeiterin oder der Mitarbeiter zu erfassen, die oder der die Maßnahme durchführt.

Die Aufnahme der oben genannten Befugnisnormen in § 186c LVwG hat zur Folge, dass die oder der Landesbeauftragte für Datenschutz gemäß § 186b Absatz 1 LVwG zu Stichproben-Kontrollen verpflichtet ist und eine Berichtspflicht gegenüber dem Landtag gemäß § 186b Absatz 2 LVwG besteht. Von der Berichtspflicht ist der IT-gestützte Abgleich gemäß § 188c Absatz 1 LVwG-Entwurf allerdings ausgenommen.

**7. Zu Nummer 7 (Einführung von §§ 188c, 188d LVwG-Entwurf):**

**a. Zu § 188c LVwG-Entwurf:**

Die neu geschaffte Vorschrift des § 188c LVwG-Entwurf führt zwei Maßnahmen zur Weiterverarbeitung verfügbarer personenbezogener Daten ein, nämlich einen niedrigschwelligen IT-gestützten Abgleich und als eingriffsintensivere Maßnahme die (automatisierte) Datenanalyse.

**b. Zu § 188c Absatz 1 LVwG-Entwurf:**

Der IT-gestützte Abgleich ist als niedrigschwelliger Abgleich konzipiert.

Es handelt sich um einen suchenden Datenabgleich zur Feststellung von Übereinstimmungen. Durch ihn werden polizeiliche Bewertungen, Prognosen und Entscheidungen nicht ersetzt. Vielmehr dient er als Instrument, das die Polizei anlassbezogen dabei unterstützen soll, im Rahmen der Sachbearbeitung – also zur Ergänzung eines bereits vorhandenen Sachverhalts – die für diese Bewertungen, Prognosen und Entscheidungen erforderlichen Tatsachenfeststellungen möglichst verlässlich zu treffen. Bei einer Begrenzung der Befugnis auf eine sehr schlichte Form des Abgleichs einer überschaubaren Zahl von Daten, die näher eingegrenzt sind, bewertete das BVerfG das besondere Eigengewicht einer solchen Maßnahme als gering (s. dazu Urt. v. 16. Feb. 2023, 1 BvR 1547/19 pp. = BVerfGE 165, 363 Rn. 72, 74, 108). Der Abgleich erlaubt nur die Suche nach einem den Suchdaten entsprechenden Gegenstück in einer anderen Datensammlung. Die Maßnahme zielt nicht auf eine Suche nach unbekannten Mustern ab.

Durch die Verweisung auf § 188a Absatz 1 und 2 LVwG und § 479 Absatz 2 Satz 2 Nummer 1 und 2 StPO soll zum Ausdruck gebracht werden, dass weder beim IT-gestützten Abgleich noch bei der Analyse nach Absatz 2 Daten zusammengeführt werden dürfen, deren Verarbeitung im Hinblick auf den jeweiligen Anlass der Maßnahme unverhältnismäßig wäre. Auch das Zusammenführen von Daten in eine Analyseplattform wird als rechtfertigungsbedürftige Datenverarbeitung angesehen. Um diese Maßgabe sowohl für die präventive als auch für die repressive Datenverarbeitung einheitlich sicherzustellen, wurde auf die genannten Vorschriften der StPO verwiesen.

**c. Zu § 188c Absatz 2 LVwG-Entwurf:**

Die automatisierte Datenanalyse geht über den IT-gestützten Datenabgleich hinaus.

Die Trennung polizeilicher Datenbestände erschwert eine umfassende Auswertung relevanter Sachverhalte hinsichtlich gemeinsamer Strukturen, Handlungsmuster, Personengruppen sowie zeitlicher, sachlicher, organisatorischer, personeller und situativer Zusammenhänge. Die Datenanalyse überwindet diese Grenze mit dem Ziel, Anhaltspunkte für Gefahren und bevorstehende Straftaten zu identifizieren, die bislang unentdeckt blieben. Dabei löst das Zusammenführen der Daten im ersten Schritt zunächst ein strukturelles Problem der polizeilichen Dateisysteme, das darin besteht, dass Informationen häufig in unterschiedlichen Formaten und in disparaten Dateien gespeichert sind und somit nicht im gleichen Bearbeitungskontext simultan verfügbar werden. Der angestrebte Analysevorgang umfasst als zweiten Schritt eine Reihe simultan ausgelöster und miteinander verknüpfter Suchaktionen, die auf Wenn-Dann-Operatoren basieren und den zusammengeführten Datenbestand durchforsten. Als regelbasierte beziehungsweise deterministi-

sche Datenanalyse folgt dieser Prozess einem klar definierten, unveränderlichen Ablauf und liefert dadurch konsistente sowie reproduzierbare Ergebnisse, die einer effektiven Gegenkontrolle zugänglich sind.

Das BVerfG erachtet es als legitimes Ziel, die in der polizeilichen Praxis bestehenden Erkenntnisgrenzen mithilfe der automatisierten Datenanalyse zu überwinden (s. BVerfG a. a. O. Rn. 70).
Der Grundsatz der Verhältnismäßigkeit fordert vom Gesetzgeber jedoch bei der Ausgestaltung der (automatisierten) Datenanalyse je nach dem Gewicht des Grundrechtseingriffs, der mit ihr einhergeht, einen angemessenen Rechtsgüterschutz und eine angemessene Eingriffsschwelle vorzusehen:

- Ermöglicht die automatisierte Anwendung einen schwerwiegenden Eingriff in die informationelle Selbstbestimmung der Betroffenen, ist dies nur unter den engen Voraussetzungen zu rechtfertigen, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten. Erforderlich ist insofern mindestens eine hinreichend konkretisierte Gefahr für besonders wichtige Rechtsgüter (BVerfG a. a. O. Rn. 104-106).
- Hingegen kann bei weniger gewichtigen Eingriffen der Kreis der schützenden Rechtsgüter weitergezogen werden; auch die Gefahrenschwelle kann dann abgesenkt werden (BVerfG a. a. O. Rn. 107).

Das unterschiedliche Eingriffsgewicht und die mit ihm korrelierenden Vorgaben zum Rechtsgüterschutz und zur Eingriffsschwelle bilden die nachfolgenden Absätze ab.

### g. Zu § 188c Absatz 3 LVwG-Entwurf:

§ 188c Absatz 3 LVwG-Entwurf regelt die Eingriffsvoraussetzungen für eine Datenanalyse mit reduziertem Eingriffsgewicht.

Für die Datenanalyse gemäß § 188c Absatz 3 LVwG-Entwurf sind die Datenquellen auf die abschließend aufgezählten Systeme sowie Daten aus Asservaten und anderen Beweismitteln beschränkt. Hinzu kommt, dass bestimmte Daten aus sehr eingriffsintensiven Maßnahmen (Wohnraumüberwachung und Online-Durchsuchung) ausgeschlossen sind (§ 188c Absatz 6 Satz 1 LVwG-Entwurf). Verkehrsdaten aus Funkzellenabfragen dürfen nur im Einzelfall händisch eingebunden werden (§ 188c Absatz 5 Satz 2 LVwG-Entwurf). Ein Bild über das Verhalten einer Person ist nur für einen kurzen Zeitraum gestattet (§ 188c Absatz 7 Satz 2 LVwG-Entwurf).
Dem reduzierten Eingriffsgewicht entspricht, dass die Eingriffsschwelle als hinreichend konkretisierte Gefahr für Rechtsgüter von mindestens „erheblichem Gewicht“ ausgestaltet werden kann (s. BVerfG a. a. O. Rn. 107).
Dieser Vorgabe entspricht auch die in § 188c Absatz 3 Satz 1 Nummer 2 LVwG-Entwurf enthaltene Eingriffsschwelle, die als Ziel der (automatisierten) Datenanalyse die Verhütung bestimmter Straftaten formuliert. Dabei wird allerdings nicht an einen abstrakten Straftatenkatalog als Kriterium angeknüpft. Dem LVwG liegt ein rechtsgutbezogener Ansatz zugrunde, wonach die Analyse zur Verhütung von Straftaten nur dann angeordnet werden darf, wenn diese Straftat ein Rechtsgut aus § 188c Absatz 3 Satz 2 LVwG-Ent-

wurf schützt. Dies beschränkt die relevanten Szenarien, in welchen die Maßnahme zur Verhütung von Straftaten angeordnet werden kann. Zusätzlich muss für das betreffende Rechtsgut mindestens eine konkretisierte Gefahr vorliegen, die in der erneuten Begehung gleichgelagerter Straftaten begründet ist. Die zusätzliche Anforderung, dass mit „weiteren, gleichgearteten Angriffen“ zu rechnen sein muss, beschränkt diese Variante auf die Verhütung von Straftaten, die regelmäßig in Serie begangen werden (vergleiche BVerfG a. a. O. Rn. 160 f.).
§ 188c Absatz 3 Satz 2 LVwG-Entwurf enthält schließlich eine abschließende Aufzählung der Rechtsgüter, zu deren Schutz die (automatisierten) Datenanalyse angeordnet werden darf. Während § 188c Absatz 3 Satz 2 Nummer 1 LVwG-Entwurf „besonders wichtige Rechtsgüter“ nennt (vergleiche BVerfG a. a. O. Rn. 105), werden in § 188c Absatz 3 Satz 2 Nummern 2 und 3 LVwG-Entwurf die Rechtsgüter von „zumindest erheblichem Gewicht“ aufgeführt (vergleiche BVerfG a. a. O. Rn. 107).

Von der vom BVerfG aufgezeigten Möglichkeit für automatisierte Datenanalysen mittlerer Schwere eine Eingriffsschwelle vorzusehen, die noch hinter einer konkretisierten Gefahr zurückbleibt (s. dazu BVerfG a. a. O. Rn. 107), macht der Entwurf keinen Gebrauch.

**h. Zu § 188c Absatz 4 LVwG-Entwurf:**

§ 188c Absatz 4 LVwG-Entwurf ermöglicht eine automatisierte Datenanalyse mit hohem Eingriffsgewicht.
Deshalb werden strenge Anforderungen an die zeitliche Nähe des befürchteten Schadens und den Rang der zu schützenden Rechtsgüter gestellt. Solche Analysen sind daher nur zur Abwehr konkreter Gefahren für besonders gewichtige Rechtsgüter (§ 188c Absatz 3 Satz 2 Nummer 1 LVwG-Entwurf) zulässig.
Der Entwurf geht damit über Vorgaben des BVerfG für automatisierte Datenanalysen hinaus; danach wäre als Eingriffsschwelle grundsätzlich auch eine hinreichend konkretisierte Gefahr ausreichend (vergleiche BVerfG a. a. O. Rn. 106).

**i. Zu § 188c Absatz 5 LVwG-Entwurf:**

Eine Reduzierung der verfügbaren Datenmenge kann auch durch die Beschränkung auf die Ergebnisse gezielter Abfragen erreicht werden, die händisch im Einzelfall einbezogen werden müssen (vergleiche BVerfG a. a. O. Rn. 88). Für extern geführte staatliche Register sieht § 188c Absatz 5 Satz 1 LVwG-Entwurf daher vor, dass - je nach Erforderlichkeit - einzelne Datensätze nur aus gezielten Abfragen in den Abgleich einbezogen werden dürfen. Hierzu zählen etwa Datensätze des Einwohnermeldeamtes oder des Ausländerzentralregisters, sofern ihre Einbeziehung für den jeweiligen Sachverhalt relevant ist.
Die Einbeziehung von Datenbeständen aus Funkzellabfragen hat, wegen der großen Anzahl von Daten potentiell unbeteiligter Personen, ein hohes Gewicht (vergleiche BVerfG a. a. O. Rn. 85). Solche Daten dürfen in eine (automatisierte) Datenanalyse, die unter den Voraussetzungen des Absatzes 3 durchgeführt wird, nur im Einzelfall händisch eingebunden werden.

**j. Zu § 188c Absatz 6 LVwG-Entwurf:**

§ 188c Absatz 6 LVwG-Entwurf schließt bestimmte Daten und Datenquellen für Datenanalysen mit reduziertem Eingriffsgewicht beziehungsweise insgesamt für alle Datenanalysen aus. Insbesondere enthält § 188c Absatz 6 Satz 2 Nummer 3 LVwG ein ausdrückliches Verbot der Anbindung der Anwendung an das Internet, da dies die automatisierte Verarbeitung einer unüberschaubar großen Zahl personenbezogener Daten Unbeteiligter zur Folge hätte (vergleiche BVerfG a. a. O. Rn. 88). Datensätze aus dem Internet beziehungsweise OSINT-Daten dürfen nur soweit erforderlich als Ergebnis gezielter Recherchen im Einzelfall (gemäß § 188c Absatz 5 Satz 1 LVwG-Entwurf) in die automatisierte Datenanalyse einbezogen werden.

**k. Zu § 188c Absatz 7 LVwG-Entwurf:**

Wird mittels einer (automatisierten) Datenanalyse das Verhalten einer Person über längere Zeit nachvollziehbar gemacht, ist der Eingriff in das Recht auf informationelle Selbstbestimmung sehr intensiv (vergleiche BVerfG a. a. O. Rn. 77). § 188c Absatz 7 Satz 1 LVwG-Entwurf knüpft daher die Erstellung eines Bewegungs- oder Verhaltensprofils an zusätzliche Voraussetzungen. Außerdem ist der Zeitraum, auf den sich Datenanalysen, die zu Zwecken im Sinne des Absatzes 3 durchgeführt werden, gemäß § 188c Absatz 7 Satz 2 LVwG-Entwurf zeitlich auf eine Woche beschränkt. Vorbild für diese zeitliche Grenze ist die kurzfristige – weniger eingriffsintensive – planmäßige Beobachtung mit Observationsmitteln (§ 185 Absatz 1 LVwG). Außerdem muss die Erstellung eines Verhaltensprofils nach § 188c Absatz 8 Satz 3 LVwG-Entwurf gesondert angeordnet werden.

§ 188c Absatz 3 Satz 3 LVwG-Entwurf schließt ein sogenanntes predictive policing aus, also völlig offene Suchvorgänge, die darauf zielen, durch statistische Methoden Aussagen über die Gefährlichkeit oder andere Eigenschaften einer Person zu gewinnen.

**l. Zu § 188c Absatz 8 LVwG-Entwurf:**

§ 188c Absatz 8 LVwG-Entwurf regelt die Anordnungsbefugnisse. Die Abstufungen spiegeln das unterschiedliche Eingriffsgewicht der Maßnahmen wider.

§ 188c Absatz 8 Satz 1 LVwG-Entwurf statuiert für den IT-gestützten Abgleich, den jede Polizeivollzugsbeamtin oder jeder Polizeivollzugsbeamte anordnen kann, eine Begründungspflicht. Die Pflicht stellt sicher, dass auch diese Maßnahme nicht anlasslos, sondern einzelfallbezogen und zielgerichtet erfolgt.

Die (automatisierte) Datenanalyse unterliegt qualifizierten Anordnungsbefugnissen: Bei reduziertem Eingriffsgewicht gemäß § 188c Absatz 3 LVwG-Entwurf erfolgt die Anordnung durch die Leiterin oder den Leiter des Landespolizeiamtes, des Landeskriminalamtes, einer Polizeidirektion oder durch von ihr oder ihm besonders beauftragte Personen des Polizeivollzugsdienstes (§ 188c Absatz 8 Nummer 1 LVwG-Entwurf in Verbindung mit § 186 Absatz 2 LVwG). (Automatisierte) Datenanalysen mit hohem Eingriffsgewicht bedürfen der richterlichen Anordnung (§ 188c Absatz 8 Satz 2 Nummer 2 LVwG-Entwurf in Verbindung mit § 186 Absatz 1 LVwG). In beiden Fällen muss die Erstellung eines Bil-

des über das Verhalten einer Person gemäß § 188c Absatz 7 LVwG-Entwurf gesondert angeordnet werden (§ 188c Absatz 8 Satz 3 LVwG-Entwurf).

**m. Zu § 188d LVwG-Entwurf:**

Der Regelungsgehalt des § 188d LVwG-Entwurf sind wesentliche methodische Aspekte der (automatisierten) Datenanalyse im Sinne von § 188c Absatz 2 LVwG-Entwurf sowie eine Ermächtigung, diese Regelungen durch eine Verwaltungsvorschrift weiter zu konkretisieren.

**n. Zu § 188d Absatz 1 LVwG-Entwurf:**

Die Beschränkung des IT-gestützten Abgleichs und der (automatisierten) Datenanalyse auf nach § 188b Absatz 1 LVwG gekennzeichnete Daten schafft die Voraussetzung für eine Anwendung des Grundsatzes der hypothetischen Datenneuerhebung. Es dürfen nur Daten zusammengeführt werden, deren Verarbeitung verhältnismäßig ist. Die Vorschrift regelt auch den Umgang mit unvollständig und gar nicht gekennzeichnete Daten.

**o. Zu § 188d Absatz 2 LVwG-Entwurf:**

Das Eingriffsgewicht einer (automatisierten) Datenanalyse ist umso höher, je offener der Suchvorgang gestaltet und je weniger er durch mit Erkenntnissen und Annahmen zu dem konkreten Sachverhalt gespeiste polizeiliche Suchmuster gesteuert wird (vergleiche BVerfG a. a. O. Rn. 93 ff.). § 188d Absatz 2 LVwG-Entwurf gewährleistet daher, dass die Suche zielgerichtet erfolgt. Das zulässige Ziel ergibt sich aus dem Anlass, welchem die Anordnung zugrunde liegt.
Angesichts der Streubreite der (automatisierten) Datenanalyse ist auch zu berücksichtigen, dass Unbeteiligte ein berechtigtes Interesse am Schutz ihrer Daten haben. Ob eine Person unbeteiligt ist, bemisst sich nicht allein an dem Umstand, dass sie bereits in polizeilichen Systemen gespeichert wurde, sondern an ihrer Nähe zu Sachverhalten, welche in der Vergangenheit gefahrenabwehrende Maßnahmen erforderlich gemacht haben. Hierzu kann bereits eine Unterscheidung nach Maßgabe des § 48 LDSG genügen.

**p. Zu § 188d Absatz 3 LVwG-Entwurf:**

Bei komplexen Formen des Datenabgleichs ist zur Gewährleistung individuellen Rechtsschutzes und aufsichtlicher Kontrolle – und der hierfür unerlässlichen Möglichkeit, Fehler zu erkennen und zu korrigieren – die Nachvollziehbarkeit der eingesetzten Algorithmen zu gewährleisten (vergleiche BVerfG a. a. O. Rn. 90).

**q. Zu § 188d Absatz 4 LVwG-Entwurf:**

Die technisch und organisatorisch gesicherte Beschränkung des Zugriffs einer begrenzten Anzahl von Mitarbeitenden und ihre besondere Qualifikation begrenzt die Eingriffsschwere (vergleiche BVerfG a. a. O. Rn. 89). Überdies wird die Polizei für den Fall der Verwendung eines Hochrisiko-KI-Systems im Sinne der KI-Verordnung auf ihre Betreiberpflichten nach Artikel 26 der KI-Verordnung hingewiesen.

**r. Zu § 188d Absatz 5 LVwG-Entwurf:**

Gemäß § 188c LVwG-Entwurf werden personenbezogene Daten anlassbezogen zu dem Zweck zusammengeführt, zur Abwehr der in § 188c Absatz 3 und 4 LVwG-Entwurf bezeichneten Gefahrenlagen respektive zur Verhütung bestimmter Straftaten beizutragen. Zur weiteren Erreichung dieses Ziels werden die zusammengeführten Daten dann im zweiten Schritt nach bestimmten Suchkriterien ausgewertet. Die Zusammenführung der personenbezogenen Daten ist nicht mehr gerechtfertigt, wenn der Zweck der Maßnahme erreicht ist oder nicht mehr erreicht werden kann. Die Erforderlichkeit ist nach Maßgabe von § 188d Absatz 5 Satz 2 LVwG-Entwurf regelmäßig zu prüfen.

Von der Zusammenführung der Daten mit dem Ziel ihrer Auswertung nach § 188c Absatz 1 LVwG-Entwurf ist die Analysefähigkeit von Daten zu unterscheiden, das heißt, dass sie – separiert – von vornherein in einem Format vorgehalten werden, welches die Zusammenführung und Analysierbarkeit ermöglicht. Die Vorwegnahme von Vorgaben oder Beschränkungen einer zeitgemäßen technischen Umsetzung, wie sie Programm Polizei 20/20 zum Ziel hat, ist nicht Gegenstand dieser Regelung.

**s. Zu § 188d Absatz 6 LVwG-Entwurf:**

Die Benachrichtigung dient der Transparenz hoheitlichen Handelns. Sie ist bei verdeckten Maßnahmen Grundvoraussetzung nachträglichen Rechtsschutzes. Im Falle der (automatisierten) Datenanalyse, die sich in der Regel nicht gegen eine bestimmte Person richtet und in die eine große Zahl personenbezogener Daten automatisiert einbezogen werden, fokussiert sich das Telos der Benachrichtigung (Nachvollziehbarkeit und Kontrolle hoheitlichen Handelns) auf die Person, über die neue Erkenntnisse erlangt werden, die wiederum Anlass für weitere polizeiliche Maßnahmen sein können.

**t. Zu § 188d Absatz 7 LVwG-Entwurf:**

Das BVerfG gestattet in der Hessen-Data-Entscheidung (Urt. v. 16. Feb. 2023, 1 BvR 1547/19 pp. = BVerfGE 165, 363), dass der Gesetzgeber die Verwaltung – wegen der besonderen Technizität und der raschen Fortentwicklungsbedürftigkeit der Anwendungen, die eine tiefergehende gesetzliche Normierung nicht praktikabel erscheinen lässt – ermächtigen darf, die nähere Regelung organisatorischer und technischer Einzelheiten in einer Verwaltungsvorschrift weiter zu konkretisieren. Dies muss in abstrakt-genereller Form geschehen und die Verwaltungsvorschrift ist zu veröffentlichen. Nach Maßgabe des Gesetzesvorbehalts muss der Gesetzgeber dabei die wesentlichen Vorgaben hinreichend bestimmt und normenklar selbst regeln (BVerfG a. a. O. Rn. 115-122).

**8. Zu Nummer 8 (Änderung von § 192 LVwG):**

Die Richtlinie (EU) 2023/977 trifft Regelungen zum Informationsaustausch zwischen den EU-Mitgliedstaaten und den Schengen assoziierten Staaten zum Zweck der Verhütung, Aufdeckung oder Untersuchung von Straftaten. Ziel ist eine Verbesserung des bestehenden Rechtsrahmens zum Informationsaustausch, um insbesondere auf grenzüberschrei-

tende kriminelle Aktivitäten reagieren zu können. Durch die Informationsaustauschrichtlinie soll ein angemessener und rascher Informationsaustausch zwischen den Mitgliedstaaten gewährleistet werden.

Mit dem Gesetz über den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (vergleiche BR-Drucksache 640/25) wird die Richtlinie auf Bundesebene vollständig und auf Ebene der Länder im Hinblick auf die Strafverfolgung umgesetzt werden.
Grundsätzlich ist vorgesehen, dass das Bundeskriminalamt für die inländischen zuständige Behörden Daten an andere Staaten übermittelt. Die vorgelagerte Datenübermittlung der Bundesländer an das Bundeskriminalamt folgt den allgemeinen Regelungen für Datenübermittlungen im Inland.
Durch den neuen § 192 Absatz 4 Satz 1 LVwG-Entwurf wird für den präventiven Bereich klargestellt, dass im Falle eines direkten Informationsaustausch zwischen der Polizei und den mit polizeilichen Aufgaben betrauten Stellen anderer Mitgliedstaaten der Europäischen Union und der Schengen assoziierten Staaten, die bestehenden Datenübermittlungsbefugnisse auch im Anwendungsbereich der Richtlinie (EU) 2023/977 Geltung beanspruchen.
Die nicht grundrechtssensiblen überwiegend verfahrensbezogenen Vorgaben der Richtlinie sollen gemäß § 192 Absatz 4 Satz 2 LVwG-Entwurf in einer Rechtsverordnung umgesetzt werden.
Der bisherige § 192 Absatz 4 LVwG wird zu § 192 Absatz 5 LVwG-Entwurf.

**9. Zu Nummer 9 (Änderung von § 195 LVwG-Entwurf):**

**a. Zu § 195 Absatz 1:**

Es handelt sich um die redaktionelle Korrektur einer Fehlverweisung.

**b. Zu § 195 Absatz 2:**

Mit § 195 Absatz 2 wird das LVwG um eine besondere Form des Abgleichs erweitert, welcher auf die Bestätigung der Identität einer Person aufgrund ihrer biometrischen Merkmale abzielt. Die Maßnahme wird dadurch charakterisiert, dass sie eine weitere Verarbeitung von Daten ermöglicht, die aufgrund anderer Rechtsgrundlagen erhoben wurden. Ein spezialgesetzlicher Regelungsbedarf besteht, da für diese Art des Abgleichs biometrische Daten von Gesichtern und Stimmen verwendet werden dürfen. Nach § 24 Absatz 3 LDSG ist die Verarbeitung biometrischer Daten nur zulässig, wenn sie ausdrücklich durch eine Rechtsvorschrift gestattet ist.

Der Abgleich nach § 195 Absatz 1 LVwG erfolgt ausschließlich auf Grundlage von Audio-, Bild- und Videodateien, welche bereits rechtmäßig in polizeilichen Datei- und Informationssystemen gespeichert wurden. Diese Voraussetzung gilt sowohl für die Referenz- als auch für die Vergleichsdaten. Zum Zwecke des Abgleichs dürfen aus diesen Daten biometrische Daten im Sinne des § 21 Nummer 12 LDSG erstellt werden und auf Übereinstimmungen geprüft werden. Das ungezielte Suchen in diesen Daten ist nicht zulässig.

Allerdings ist es auch nicht erforderlich, dass eine Person, deren Daten als Referenzdaten abgeglichen werden, bereits namentlich bekannt ist. Das Ziel der Bestätigung der Identität wird gewährleistet, wenn sich aus den Vergleichsdaten Übereinstimmungen und Daten zur Person ergeben. Ausreichend ist, dass eine Person aufgrund biometrische Referenzdaten eindeutig identifizierbar ist.

Gegenüber dem „einfachen“ Datenabgleich nach § 195 Absatz 1 LVwG ist § 195 Absatz 2 LVwG-Entwurf insoweit an strengere Voraussetzungen gekoppelt, als der „biometrische“ Datenabgleich nach dieser Vorschrift nicht zur polizeilichen Aufgabenerfüllung insgesamt, sondern nur zur Abwehr einer Gefahr für die öffentliche Sicherheit zugelassen ist. Damit sind zum Beispiel Gefahrenerforschungsmaßnahmen und Vollzugs- und Ermittlungshilfe ausgeschlossen. Darüber hinaus muss der Abgleich grundsätzlich darauf gerichtet sein, die Person, die für die Gefahr verantwortlich ist, anhand der in polizeilichen Datei- und Informationssystemen rechtmäßig gespeicherten Daten zu identifizieren. Sie kann auch zum Ziel haben auf diese Weise die Identität einer gefährdeten Person zu bestätigen, jedoch muss in diesem Fall eine „erhebliche Gefahr“ vorliegen. Ein erhebliche Gefahr ist eine Gefahr für ein bedeutsames Rechtsgut wie den Bestand oder Sicherheit des Bundes oder eines Landes, das Leben, die Gesundheit, die Freiheit, nicht unwesentliche Vermögenswerte sowie andere strafrechtlich geschützte Güter von vergleichbarem Gewicht (Graulich in Lisken/Denninger, PolR-HdB, 7. Aufl. 2021, E. Rn. 150).
Der besonderen Sensibilität biometrischer Daten wird zudem dadurch Rechnung getragen, dass die Maßnahme zwingend erforderlich sein muss. Diese Formulierung orientiert sich an § 24 Absatz 1 LDSG. Die Verarbeitung biometrischer Daten ist zwingend erforderlich, wenn die Durchführung der Maßnahme im konkreten Einzelfall unverzichtbar ist, um Gefahren für die öffentliche Sicherheit abzuwehren. Selbst wenn eine zwingende Erforderlichkeit aus Gründen eines erheblichen öffentlichen Interesses gegeben ist, darf die Verarbeitung nur erfolgen, sofern die Interessen des Verantwortlichen an der Datenverarbeitung in einem angemessenen Verhältnis zum verfolgten Zweck stehen und der Wesensgehalt des Rechts auf Datenschutz gewahrt bleibt.
Schließlich dürfen Daten aus dem Einsatz technischer Mittel in Wohnungen und durch den verdeckten Zugriff auf informationstechnische Systeme gewonnene Daten für den Abgleich – vorbehaltlich der besonderen Vorschrift § 188a Absatz 3 LVwG – nicht herangezogen werden.
In formaler Hinsicht setzt der biometrische Datenabgleich nach § 195 Absatz 2 LVwG-Entwurf eine schriftlich begründete Entscheidung voraus. Die Vorschriften über die Durchführung der nachträglichen Fernidentifizierung gemäß § 195c LVwG-Entwurf gelten weitgehend entsprechend. Wird ein Hochrisiko-KI-System im Sinne der KI-Verordnung eingesetzt, sind die Vorgaben der KI-Verordnung zu beachten.

### 10. Zu Nummer 10 (Einführung von §§ 195b, 195c LVwG-Entwurf):

### a. Zu § 195b LVwG-Entwurf:

Mit § 195b LVwG-Entwurf wird eine Rechtsgrundlage zur nachträglichen biometrischen Fernidentifizierung unter Verwendung öffentlich zugänglicher Daten des Internets eingeführt (vergleiche zum Begriff: Allgemeiner Teil Punkt II.).

**b. Zu § 195b Absatz 1 LVwG-Entwurf:**

§ 195b Absatz 1 Satz 1 und 2 LVwG-Entwurf gestattet eine Fernidentifizierung mittels biometrischer Daten durchzuführen, die aus öffentlich zugänglichen Daten des Internets gewonnen wurden.

Der grundlegende Unterschied im Verhältnis zum „biometrischen“ Datenabgleich nach § 195 Absatz 2 LVwG-Entwurf besteht darin, dass dieser sich auf Daten beschränkt ist, die aufgrund anderer Anlässe bereits rechtmäßig gespeichert wurden, während § 195b Absatz 1 LVwG-Entwurf die gezielte Erhebung von Vergleichsmaterial zur Durchführen der biometrischen Fernidentifizierung ermöglicht. Die Vorschrift enthält dazu in § 195b Absatz 1 Satz 3 LVwG-Entwurf eine eigene Rechtsgrundlage, welche die automatisierte Erhebung und Speicherung personenbezogener Daten aus den öffentlich zugänglichen Bereichen des Internets zum Zwecke des Abgleichs erlaubt, und gestattet diese für den biometrischen Abgleich zu verwenden. Zu den Daten, die aus dem Internet gewonnen werden dürfen, zählen Daten, die von jedermann verwendet werden können (beispielsweise aus sozialen Medien), sofern sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten.

Die nachträgliche biometrische Fernidentifizierung gemäß § 195b LVwG-Entwurf dient – wie die biometrische Echtzeit-Fernidentifizierung (§ 184b LVwG-Entwurf) – ausschließlich dem Ziel der Bestätigung der Identität einer bestimmten Person. Andere Verarbeitungszwecke, zum Beispiel eine Profilbildungen, sind nicht zugelassen. Das heißt das Abgleichergebnis kann nur in der Feststellung der Übereinstimmung zwischen der Person, von der die biometrischen Referenzdaten stammen, mit einer Person, deren biometrische Daten aus öffentlich zugänglichen Quellen des Internets gewonnen wurden, bestehen. Unberührt bleibt freilich die Weiterverarbeitung des Abgleichergebnisses nach anderen Vorschriften.

Die Eingriffsvoraussetzungen des § 195b Absatz 1 LVwG-Entwurf sind gegenüber § 195 Absatz 2 LVwG-Entwurf deutlich erhöht. Das gilt sowohl für die Rechtsgüter, deren Schutz die Maßnahmen zu dienen hat, als auch für die Eingriffsschwelle. Die nachträgliche biometrische Fernidentifizierung, die als Referenzmaterial öffentlich zugängliche Daten zu Stimmen und Gesichtern aus dem Internet zulässt, muss der Abwehr einer konkreten Gefahr für Rechtsgüter dienen, die nach der Rechtsprechung des BVerfG zu den „besonders wichtigen Rechtsgütern“ zählen (zu diesem Bgriff: BVerfG, Urt. v. 16. Feb. 2023, 1 BvR 1547/19 = BVerfGE 165, 363 Rn. 105 m. w. N.).
Nach der Rechtsprechung des BVerfG muss eine Rechtsgrundlage, welche die Erhebung einer großen Datenmenge potenziell unbeteiligter Personen zum Zweck eines Abgleichs gestattet, der Abwehr konkreter Gefahren für hochrangige Rechtsgüter dienen (BVerfG, Beschl. 4. Apr. 2006, 1 BvR 518/03 = BVerfGE 115, 320, 360 ff.; BVerfG, Urt. 20. Apr. 2016, 1 BvR 966/09 pp. = BVerfGE 141, 202 Rn. 207). Eine hinreichend konkretisierte Gefahr würde nicht genügen (instruktiv BVerfG, Beschl. v. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE 165, 1 Rn. 185 ff.). Die zur Rasterfahndung formulierten Grundsätze gelten für eine Fernidentifizierung, die sich des Internets als Datenquelle bedient, entsprechend. Der Umstand, dass öffentlich zugängliche personenbezogene Daten verwendet werden, führt zu keiner anderen Bewertung, da dieser Umstand nichts an der Tatsa-

che ändert, dass auch bei der Gewinnung solcher Daten das die Rasterfahndung prägende Merkmal erfüllt ist. Dies besteht darin, dass die einbezogenen Daten keinen Bezug zur Gefahrenlage haben, die Maßnahme für die Betroffenen mithin anlasslos ist (vergleiche BVerfG a. a. O.).

§ 195b Absatz 1 LVwG ist (auch im Falle des Einsatzes eines KI-Systems im Sinne der KI-Verordnung) mit Artikel 5 Absatz 1 Buchstabe e der KI-Verordnung vereinbar. Die genannte Vorschrift der KI-Verordnung verbietet die Verwendung „von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet erstellen“.
Das Verbot aus Artikel 5 Absatz 1 Buchstabe e der KI-Verordnung bezieht sich ausdrücklich darauf, dass durch das „ungezielte Auslesen von Gesichtsbildern“ keine „Datenbanken zur Gesichtserkennung“ erstellt werden dürfen. Der einschlägige Erwägungsgrund 43 der KI-Verordnung begründet das Verbot inhaltlich übereinstimmend damit, dass die Verwendung solcher KI-Systeme das Gefühl der Massenüberwachung verstärken. Der Begriff „ungezieltes Auslesen“ steht in der KI-Verordnung mithin für das massenhafte, wahllose Extrahieren von Gesichtsbildern, mit dem Ziel biometrischer Datenbanken zu erstellen, die für verschiedenste Anlässe und Zwecke genutzt werden können. Eine Verarbeitung von öffentlich zugänglichen Daten wird dagegen von dem Verbot des Artikel 5 Absatz 1 Buchstabe e nicht erfasst, sofern Gesichtsbilder nur anlassbezogen gewonnen werden und nur für diesen Anlass verarbeitet werden, nicht aber auch für zukünftige Verarbeitungsvorgängen in einer Datenbank vorrätig gehalten werden. Diese Schranken werden durch das Regelungsgefüge von §§ 195b und 195c LVwG-Entwurf gewahrt:
Der Grundgedanke des § 195b Absatz 1 LVwG-Entwurf ist, dass ein bestimmter Sachverhalt vorliegt, der die Abwehr einer konkreten Gefahr für Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person oder den Bestand oder die Sicherheit des Bundes oder eines Landes zum Gegenstand hat. Zu diesem individuellen Anlass darf die Polizei Daten aus dem Internet automatisiert verarbeiten, um biometrische Vergleichsdaten für den Abgleich zu gewinnen. Die aus dem Internet gewonnenen Daten werden dabei gemäß § 195c Absatz 1 Satz 1 LVwG-Entwurf ausschließlich zweckgebunden respektive gebunden an den vorgenannten individuellen Erhebungsanlass gespeichert. Eine Verwendung der gespeicherten Daten zu anderen Zwecken beziehungsweise neuen, zukünftigen Anlässen – wie es der Grundidee einer „Datenbank“ entspräche – ist ausdrücklich ausgeschlossen. Hinsichtlich dieses umfassend gegen andere Nutzung abgeschirmten Datensatzes wird der Abgleich in Bezug auf die in § 195b Absatz 2 LVwG-Entwurf genannten Person durchgeführt. § 195c Absatz 1 Satz 3 LVwG-Entwurf sieht schließlich vor, dass die zum Zwecke des Abgleichs erlangten öffentlich zugänglichen personenbezogenen Daten unverzüglich zu löschen sind, wenn nach Durchführung des Abgleichs und menschlicher Bestätigung des Ergebnisses keine weiteren polizeilichen Maßnahmen getroffen werden sollen.

### c. Zu § 195b Absatz 2 LVwG-Entwurf:

§ 195b Absatz 2 LVwG-Entwurf enthält ergänzende Voraussetzungen für die Anordnung einer nachträglichen biometrischen Fernidentifizierung gemäß § 195b Absatz 1 LVwG-Entwurf.

Die nachträgliche biometrische Fernidentifizierung richtet sich gegen die Person, deren Daten zu Gesicht und Stimme Ausgangspunkt die Referenzdaten des biometrischen Abgleichs bilden. Diese Daten dürfen auf Übereinstimmung mit Vergleichsdaten abgeglichen werden. § 195b Absatz 2 Satz 1 LVwG-Entwurf bestimmt, dass grundsätzlich nur Daten solcher Personen im Rahmen des § 195b LVwG-Entwurf abgeglichen werden dürfen, von denen die Gefahr für die Rechtsgüter ausgeht, zu deren Schutz die Maßnahme erforderlich ist. Abweichend hiervon kann die Maßnahme nach § 195b Absatz 2 Satz 2 LVwG-Entwurf auch zum Schutz einer Person durchgeführt werden, deren Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung konkret gefährdet sind, zum Beispiel zur Suche von Opfern einer Entführung, des Menschenhandels oder sexueller Ausbeutung sowie zur Erlangung von Hinweisen auf den Aufenthaltsort vermisster Personen.

Hochrisiko-KI-Systeme im Sinne der KI-Verordnung unterliegen einem speziellen Regelungsregime. Insbesondere Artikel 26 der KI-Verordnung normiert bestimmte Pflichten für den Betreiber eines Hochrisiko-KI-Systems. Sie treffen auch die Polizei, soweit diese ein Hochrisiko-KI-System in eigener Verantwortung verwendet (vergleiche Artikel 3 Nummer 4 der KI-Verordnung).
Artikel 26 Absatz 10 Unterabsatz 3 der KI-Verordnung schreibt Einsatzziele für den Fall vor, dass ein Hochrisiko-KI-System zu Zwecken der Strafverfolgung eingesetzt wird. Unter Strafverfolgung im Sinne der KI-Verordnung ist auch eine Tätigkeit zu verstehen, die auf die Verhütung von Straftaten zielt, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (vergleiche Artikel 3 Nummer 46 der KI-Verordnung).
Nach Artikel 26 Absatz 10 Unterabsatz 3 Satz 1 der KI-Verordnung darf ein zu Strafverfolgungszwecken eingesetztes Hochrisiko-KI-System zur nachträglichen biometrischen Fernidentifizierung in keinem Fall in nicht zielgerichteter Weise verwendet werden. Außerdem ist jeder Einsatz untersagt, der nicht in einem Zusammenhang mit einer Straftat, einem Strafverfahren, einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr einer Straftat oder der Suche nach einer bestimmten vermissten Person steht. Bei der Verwendung eines Hochrisiko-KI-Systems zur nachträglichen biometrischen Fernidentifizierung müssen diese Voraussetzungen – neben den Voraussetzungen des § 195b Absatz 1 LVwG – geprüft werden. Ihnen dürfte jedoch in der Regel keine eigenständige Bedeutung zukommen.
Ferner dürfen nach Artikel 26 Absatz 10 Unterabsatz 3 Satz 1 der KI-Verordnung keine Entscheidungen und Maßnahmen durch die Polizei ausschließlich auf der Grundlage der Ausgabe des zur nachträglichen biometrischen Fernidentifizierung eingesetzten Hochrisiko-KI-Systems getroffen werden. Dies sichert im Falle einer Maßnahme nach § 195b Absatz 1 LVwG-Entwurf die Vorschrift des § 195c Absatz 1 Satz 2 LVwG-Entwurf ab.

**d. Zu § 195b Absatz 3 LVwG-Entwurf:**

Die Anordnungsbefugnis beruht auf dem prognostizierten Eingriffsgewicht der jeweiligen Maßnahme.
Für eine nachträgliche biometrische Fernidentifizierung, die nach § 195b Absatz 1 LVwG-Entwurf auf Daten aus dem Internet rekurriert, bedarf es einer richterlichen Anordnung, die, wie die Rasterfahndung (§ 195a Absatz 2 LVwG), die Antragsstellung durch die Amts- oder Behördenleitung oder eine hierzu besonders beauftragte Person des Polizei-

vollzugsdienstes voraussetzt (Satz 1). Im Einzelnen gelten die allgemeinen Vorschriften bei Gefahr im Verzug sowie zu Begründungserfordernissen, Zuständigkeiten und Verfahren aus § 186 LVwG entsprechend (Satz 2).
Artikel 26 Absatz 10 Unterabsatz 1 und 2 der KI-Verordnung schreiben zwar bei der Verwendung eines Hochrisiko-KI-Systems zur nachträglichen biometrischen Fernidentifizierung in bestimmten Fällen eine Genehmigung durch eine Justiz- oder Verwaltungsbehörde vor. Von der Regelung ist dagegen nur der Einsatz eines solchen Systems „im Rahmen von Ermittlungen zur gezielten Suche einer Person, die der Begehung einer Straftat verdächtigt wird oder aufgrund einer solchen verurteilt wurde“ vorgesehen. Zu diesem – im Sinne der deutschen Rechtsordnung: repressiven – Zweck darf § 195b LVwG-Entwurf nicht zum Einsatz kommen.

**e. Zu § 195b Absatz 4 LVwG-Entwurf:**

§ 195b Absatz 4 LVwG-Entwurf beschreibt die Mechanismen zum Schutz des Kernbereichs privater Lebensgestaltung bei der Erlangung von öffentlich zugänglichen Daten.

**f. Zu § 195c LVwG-Entwurf:**

§ 195c LVwG-Entwurf enthält Regelungen für die Durchführung der nachträglichen Fernidentifizierung nach § 195b LVwG-Entwurf.

**h. Zu § 195c Absatz 1 LVwG-Entwurf:**

§ 195c Absatz 1 LVwG-Entwurf trifft wichtige Vorkehrungen zum Grundrechtsschutz bei der Durchführung der nachträglichen Fernidentifizierung nach § 195b LVwG-Entwurf.

Zuvörderst normiert § 195c Absatz 1 Satz 1 LVwG-Entwurf eine strenge Zweckbindung der verarbeiteten biometrischen und der aus dem Internet gewonnenen Daten. Diese bezieht sich nicht nur auf den Zweck der Datenerhebung, also die Abwehr von Gefahren für bestimmte besonders wichtige Rechtsgüter, sondern auch auf den konkreten Sachverhalt, der Anlass für die Durchführung der Maßnahme war. Damit ist sowohl die zweckkonforme Nutzung nach § 188a Absatz 1 LVwG als auch die zweckändernde Weiterverarbeitung nach § 188a Absatz 2 LVwG ausgeschlossen. Auf diese Weise wird das Entstehen einer (unspezifischen) Datenbank ohne konkreten Fallbezug unterbunden.
Um die Beeinträchtigung Unbeteiligter zu reduzieren, dürfen außerdem allein auf Grundlage des von der Anwendung angebotenen Abgleichergebnisses keine Folgemaßnahmen getroffen werden. Vielmehr bedarf es stets einer menschlichen Prüfung des Abgleichergebnisses. Dies entspricht der Vorgabe aus Artikel 26 Absatz 10 Unterabsatz 3 Satz 1 der KI-Verordnung, dass eine Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, nicht ausschließlich auf der Grundlage der Ausgabe des Systems zur nachträglichen biometrischen Fernidentifizierung getroffen werden darf. Artikel 14 Absatz 5 Unterabsatz 1 der KI-Verordnung sieht für Hochrisiko-KI-Systeme vor, dass eine Überprüfung des Identifizierungsvorgangs von zwei entsprechend qualifizierten natürlichen Personen vorzunehmen ist. Zwar kann von dieser Vorgabe gemäß Artikel 14 Absatz 5 Unterabsatz 2 der KI-Verordnung abgewichen werden, die in den Bereichen Strafverfolgung, Migration, Grenzkontrolle oder Asyl verwendet werden. Die Voraussetzung

hierfür – dass nämlich die Überprüfung durch zwei Beschäftigte „unverhältnismäßig wäre“ – lässt sich für die herausgehobenen Einsatzszenarien, die § 195b LVwG-Entwurf im Blick hat, nicht begründen.
Die menschliche Prüfung nach § 195c Absatz 1 Satz 2 LVwG-Entwurf stellt zugleich das auslösende Moment für die Befugnis dar, die zum Zwecke des Abgleichs zusammengeführten Daten weiterhin in den polizeilichen Systemen zu speichern. Ergibt die Prüfung, dass auf Grundlage des Abgleichergebnisses weitere Maßnahmen erforderlich sind, dürfen die mit dieser Entscheidung zusammenhängenden Daten nach den allgemeinen Regeln zur Aufgabenerfüllung gespeichert werden. Für alle anderen Daten besteht ein uneingeschränktes Verarbeitungsverbot. Sie sind zu löschen.

**h. Zu § 195c Absatz 2 LVwG-Entwurf:**

Die Benachrichtigung über die Durchführung einer nachträglichen Fernidentifizierung gemäß § 195b Absatz 1 LVwG-Entwurf dient der Transparenz hoheitlichen Handelns. Sie ist bei eingriffsintensiven verdeckten Maßnahmen Grundvoraussetzung des Rechtsschutzes.

**i. Zu § 195c Absatz 3 LVwG-Entwurf:**

§ 195c Absatz 3 trifft Regelungen zur Transparenz und zur Nachvollziehbarkeit grundrechtsintensiven Handelns.
Zu demselben Zweck wird § 195b LVwG-Entwurf in den Kanon der Vorschriften zur Protokollierung bestimmter eingriffsintensiver Maßnahmen nach § 186c LVwG aufgenommen. § 195c Absatz 3 Satz 2 LVwG-Entwurf normiert darüber hinaus bestimmte spezielle Protokollierungspflichten. Über die in § 186c LVwG vorgeschriebene Protokollierung hinaus sind die eingesetzte automatisierte Anwendung zur Datenverarbeitung und die Mitarbeiterin oder der Mitarbeiter zu erfassen, die oder der die Maßnahme durchführt.
Die Aufnahme des § 195b LVwG-Entwurf in § 186c LVwG hat auch zur Folge, dass die oder der Landesbeauftragte für Datenschutz gemäß § 186b Absatz 1 LVwG zu Stichproben-Kontrollen berechtigt ist und eine Berichtspflicht gegenüber dem Landtag gemäß § 186b Absatz 2 LVwG besteht.
Die Polizei wird überdies im Falle der Verwendung eines Hochrisiko-KI-Systems im Sinne der KI-Verordnung auf ihre Betreiberpflichten nach Artikel 26 der KI-Verordnung hingewiesen.
Soweit eine tiefergehende gesetzliche Normierung wegen der besonderen Technizität und der raschen Fortentwicklungsbedürftigkeit von automatisierten Anwendungen zur Datenverarbeitung nicht praktikabel ist, hat das BVerfG dem Gesetzgeber gestattet, die Verwaltung zu ermächtigen, die nähere Regelung organisatorischer und technischer Einzelheiten in einer Verwaltungsvorschrift weiter zu konkretisieren (Urt. v. 16. Feb. 2023, 1 BvR 1547/19 pp. = BVerfGE 165, 363 Rn. 112 ff.). Nach Maßgabe des Gesetzesvorbehalts muss der Gesetzgeber aber die wesentlichen Vorgaben hinreichend bestimmt und normenklar selbst regeln.

### 11. Zu Nummer 11 (Änderung von § 200 LVwG):

Durch den Verweis auf die Regelung des § 205 Absatz 2 LVwG-Entwurf wird der Regelungsgehalt des bisherigen § 200 Absatzes 2 LVwG konkreter gefasst und die Regelungsdichte erhöht. Gleichzeitig wird durch diesen Verweis eine Vereinheitlichung der Vorschriften, die freiheitsentziehende Maßnahmen beinhalten, erreicht.
Auch für den Richtervorbehalt im Fall der Freiheitsentziehung im Zusammenhang mit einer Vorführung hat die neu geschaffene Regelung des § 205a LVwG-Entwurf Leitbildfunktion.

### 12. Zu Nummer 12 (Änderung von § 201a LVwG):

§ 201a Absatz 6 Satz 7 LVwG verpflichtet die Beratungsstellen der Täterarbeit dazu, der Polizei oder einem mit der Sache befassten Gericht auf Aufforderung mitzuteilen, ob die Person, von der die Gefahr ausgeht, ein Beratungsangebot (nach § 201a Absatz 6 Satz 1 Nummer 2, Satz 4 LVwG) angenommen hat. Diese Information kann für die Polizei oder das Gericht von Bedeutung für die Gefahrenprognose und gegebenenfalls weitere Maßnahmen zum Opferschutz sein. Allerdings besteht zwischen dieser Pflicht und der Pflicht aus § 201 Absatz 6 Satz 6 LVwG, die übermittelten Daten im Falle einer Ablehnung der Beratung zu löschen, ein Spannungsverhältnis. Diese Friktion löst die Änderung des § 201a Absatz 6 Satz 7 LVwG-Entwurf auf, indem die Beratungsstellen der Täterarbeit nach dieser Vorschrift künftig berechtigt und verpflichtet werden, die Daten der Person, die eine Beratung abgelehnt hat, sowie die Umstände der Ablehnung ein Jahr lang zu speichern.
Eine darüber hinausgehende Erweiterung erfährt die Vorschrift dadurch, dass Täter-Beratungsstellen künftig nicht nur Gerichten, bei denen Anträge zum Schutz von Opfern auf Grundlage des LVwG anhängig sind, auf Aufforderung mitzuteilen haben, ob das Beratungsangebot angenommen wurde, sondern auch den mit Gewaltschutzsachen befassten Familiengerichten diese Auskunft zu erteilen haben.

### 13. Zu Nummer 13 (Änderung von § 201b LVwG)

Entsprechend der im Allgemeinen Teil dargestellten systematischen Neuordnung der Befugnisnormen zur elektronischen Aufenthaltsüberwachung übernimmt § 201b LVwG-Entwurf künftig den Anwendungsbereich des § 201c LVwG. Erfasst sind Fälle, in denen die elektronische Aufenthaltsüberwachung zur Abwehr einer hinreichend konkretisierten Gefahr für besonders wichtige Individualrechtsgüter unerlässlich ist.

#### a. Zu § 201b Absatz 1 LVwG-Entwurf:

Der Eingriffstatbestand des § 201b Absatz 1 Satz 1 LVwG-Entwurf hat – im Verhältnis zu § 201c LVwG – unverändert drei Voraussetzungen: Erstens muss von der Person, deren Aufenthalt elektronisch überwacht werden soll, eine hinreichend konkretisierte Gefahr eines schwerwiegenden Angriffs auf bestimmte, besonders wichtige Rechtsgüter – Leben, Leib und Freiheit oder die sexuelle Selbstbestimmung einer Person – ausgehen. Zwei-

tens muss die Gefahrenprognose mit dem Überwachungsziel funktionell verknüpft sein. Das heißt: Es ist zur Abwehr der Gefahrenlage erforderlich, fortlaufend zu überwachen, dass die überwachte Person nicht bestimmte Orte aufsucht, weil sich die Gefahren gerade in diesem Fall zu realisieren drohen. Und drittens muss die elektronische Aufenthaltsüberwachung respektive die mit ihr verbundene sofortige Alarmierung der Polizei zur Abwehr des Schadenseintritts unbedingt erforderlich (unerlässlich) sein, weil andere Mittel zur Überwachung fehlen oder nicht gleich geeignet sind.
§ 201b Absatz 1 Satz 1 LVwG-Entwurf unterscheidet sich von § 201c LVwG allerdings darin, dass der Tatbestand nicht erfordert, dass die Maßnahme zum Schutz einer *bestimmten* Person erfolgt. Dadurch ergibt sich die Möglichkeit, die Maßnahme auch dann anzuwenden, wenn der Kreis der gefährdeten Person nicht individuell, sondern nur anhand bestimmten Kriterien oder Gruppenzugehörigkeiten bestimmbar ist. § 201b Absatz 1 Satz 2 LVwG-Entwurf stellt dies klar. In Betracht kommt die elektronische Aufenthaltsüberwachung etwa bei einem Störer, von dem Gefahren für die sexuelle Selbstbestimmung von Kindern ausgehen; hier könnten bestimmte Orte, wie Spielplätze oder Schulen, im Umkreis um den Wohnort des Störers überwacht werden. Ähnliches gilt, wenn eine Gefahr in Bezug auf Teilnehmer bestimmter Veranstaltungen besteht.

Ungeachtet dieser Erweiterung des Eingriffstatbestandes bleibt (im Bereich des Individualrechtsgüterschutzes) der Schutz bestimmter Personen bei Hochrisikofällen häuslicher Gewalt oder gleichgelagerten Stalking-Fällen der wichtigste Anwendungsfall der elektronischen Aufenthaltsüberwachung. Dies stellt § 201b Absatz 1 Satz 3 LVwG-Entwurf heraus, indem die Fallkonstellation, die aktuell im Fokus des § 201c LVwG-Entwurf steht, als Anwendungsbeispiel („insbesondere“) hervorgehoben wird. Die elektronische Aufenthaltsüberwachung ist in den einschlägigen Fällen ein wirksames Mittel, um polizeiliche Verfügungen oder richterliche Anordnungen zu überwachen und damit zu ihrer Durchsetzung beizutragen, mit denen die Person auf Abstand gehalten werden soll, von der eine Gefahr für das Opfer häuslicher Gewalt oder Nachstellung ausgeht.
Zwischen Maßnahmen nach § 201a Absatz 1 Satz 1, Absatz 2 oder 4 LVwG (und gegebenenfalls auch solchen nach § 201 Absatz 2 oder 3 LVwG) sowie gleichgerichteten Anordnungen nach dem Gewaltschutzgesetz einerseits und der elektronischen Aufenthaltsüberwachung andererseits besteht dabei ein funktionaler Zusammenhang: In aller Regel setzt die Anordnung der elektronischen Aufenthaltsüberwachung ein Betretungs-, Kontakt- oder Näherungsverbot oder vergleichbare Maßnahmen voraus. Anderenfalls wäre die elektronische Aufenthaltsüberwachung dann nicht erforderlich respektive unerlässlich, weil weniger eingriffsintensive Mittel nicht ausgeschöpft sind. Allerdings ist die elektronische Aufenthaltsüberwachung nicht tatbestandlich daran gebunden, dass eines der genannten Verbote (noch) besteht. Vielmehr bedarf es bei Wegfall des Betretungs-, Kontakt- oder Näherungsverbots oder einer vergleichbaren Maßnahme einer (gerichtlichen) Aufhebungsentscheidung. Dies gilt für den neu gefassten Tatbestand des § 201b Absatz 1 LVwG-Entwurf unverändert fort. Eine tatbestandliche Verknüpfung hätte unausweichlich Wirksamkeitsdefizite zur Folge, wie sie in der Gesetzesbegründung zu § 201c LVwG dargestellt sind (LT-Drucksache 20/2746, S. 33 f.).“

### b. Zu § 201b Absatz 2 bis 7 LVwG-Entwurf:

Die bisherigen weitergehend deckungsgleichen Regelungen von § 201b Absatz 3 bis 9 LVwG und § 201c Absatz 3 bis 7 LVwG werden zusammengeführt mit Ausnahme der Vorschriften über das Anordnungsverfahren (bisher: § 201b Absatz 7 und 8 LVwG und § 201c Absatz 3 LVwG). Das Verfahren zur Anordnung der elektronischen Aufenthaltsüberwachung wird nunmehr in einem neuen § 201d LVwG-Entwurf geregelt und in Teilen neu gestaltet.

Neu eingeführt wird die Möglichkeit, die durch die elektronische Aufenthaltsüberwachung erlangten Daten zum Zweck der Vorbereitung und Durchführung der Abschiebung der zu überwachenden Person weiterzuverarbeiten (§ 201b Absatz 6 Satz 1 Nummer 4 LVwG-Entwurf). Dies kann insbesondere bei ausländischen Mehrfach- und Intensivstraftätern von Bedeutung sein. Die Weiterverarbeitung schließt die Nutzung der Daten zur Ermöglichung von Botschaftsvorführungen, Festnahmen zur Durchführung der Abschiebehaft oder des Abschiebegewahrsams sowie für Abschiebemaßnahmen selbst ein.
Die Tatbestandsvoraussetzungen der Weiterverarbeitungsbefugnis entsprechen denen, des Zuständigkeitsübergangs an die Zentralstelle für die Bearbeitung von Gefährdern und Straftäter im Landesamt für Zuwanderung und Flüchtlinge gemäß § 3 Absatz 8 Satz 2 Nummer 2 und 3 der Ausländer- und Aufnahmeverordnung. Da die Verwendung der Daten „zur Vorbereitung und Durchführung einer Abschiebung der überwachten Person“ erforderlich sein muss, ist hierfür in materieller Hinsicht vorauszusetzen, dass die Abschiebung der überwachten Person durchführbar ist und keine rechtlichen Abschiebungshindernisse vorliegen.

## 14. Zu Nummer 14 (Änderung von § 201c LVwG)

Das bisherige Einsatzspektrum des § 201b LVwG ist auf Fälle beschränkt, in denen eine Gefahrenlage hinsichtlich Straftaten mit terroristischem Bezug (namentlich §§ 89a, 89b, 129a oder 129b Strafgesetzbuch/StGB) besteht. Diese Schutzrichtung übernimmt § 201c LVwG-Entwurf. Der neue Tatbestand orientiert die Eingriffvoraussetzungen allerdings enger an den Vorgaben der Rechtsprechung des BVerfG.

### a. Zu § 201c Absatz 1 LVwG-Entwurf:

Eine elektronische Aufenthaltsüberwachung kann gemäß § 201c Absatz 1 LVwG-Entwurf gegenüber einer Person angeordnet werden, deren individuelles Verhalten eine konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines übersehbaren Zeitraums eine „terroristische Straftat“ begehen wird und die Überwachung des Aufenthaltsortes dieser Person unerlässlich ist, um die Straftat zu verhindern.

Den Ausgangspunkt für diese Eingriffsschwelle bildet die in der Entscheidung des BVerfG vom 20. April 2016 (1 BvR 966/09 pp. = BVerfGE 141, 220) zum Bundeskriminalamtsgesetz aufgestellte Maxime, dass der Gesetzgeber von Verfassungs wegen nicht von vornherein für jede Art der Aufgabenwahrnehmung auf die Schaffung von Eingriffstatbeständen beschränkt ist, die dem tradierten sicherheitsrechtlichen Modell der Abwehr

konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen. Vielmehr kann er die Grenzen für bestimmte Bereiche mit dem Ziel schon der Straftatenverhütung auch weiter ziehen, indem er die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert (BVerfG a. a. O. Rn. 112). Eine solche – gegenüber der konkreten Gefahr abgrenzte – hinreichend *konkretisierte* Gefahr in diesem Sinne kann danach schon bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Erforderlich ist dafür im Grundsatz, dass Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, dass eine relevante Rechtsgutsverletzung verkörpert (BVerfG a. a. O. 112; ferner: BVerfG, Beschl. v. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE 165, 1 Rn. 90 f.).
Speziell in Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können die Anforderungen an die Erkennbarkeit des Geschehens weiter abgesenkt werden, wenn dafür bereits genauere Erkenntnisse über die beteiligten Personen bestehen. Hier gilt, dass Überwachungsmaßnahmen auch dann erlaubt werden können, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, dafür aber das individuelle Verhalten einer Person bereits die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird (BVerfG a. a. O.; vergleiche auch BayVerfGH, Entscheidung v. 13. März 2025, Vf. 5-VIII-18 pp., Rn. 184 bis 187).
Allerdings ist dem Gesetzgeber – wie das BVerfG in seinem Beschluss zum Sicherheits- und Ordnungsrecht des Landes Mecklenburg-Vorpommern vom 9. Dezember 2022 (1 BvR 1345/21 = BVerfGE 165, 1) klargestellt hat – eine Grenze dabei gesetzt, an welche Straftaten er anknüpft. Problematisch sind hier insbesondere sogenannte Vorfeldtatbestände, bei denen die Strafbarkeitsschwelle durch die Einbeziehung von Vorbereitungshandlungen in das Vorfeld von Gefahren für Rechtsgüter verlagert werden. Zwar kann auch mit der Verwirklichung eines Vorfeldstraftatbestandes eine konkretisierte oder konkrete Gefahr für die jeweils geschützten Rechtsgüter einhergehen. Sicher ist dies jedoch nicht; allein aus der Gefahr der Verwirklichung eines Vorfeldstraftatbestandes ergeben sich nicht notwendigerweise bereits solche Gefahren für das Rechtsgut. Gerade auf eine Gefahr für das Rechtsgut kommt es aber nach dieser Rechtsprechung an (BVerfG a. a. O. Rn. 92).

Um den dargestellten Anforderungen besser gerecht zu werden, knüpft § 201c Absatz 1 LVwG-Entwurf die Eingriffsschwelle an einen neu einzuführenden Begriff der „terroristischen Straftat“. Diesen Begriff definiert § 201c Absatz 1 Satz 2 LVwG-Entwurf – in Übereinstimmung mit § 5 Absatz 1 Satz 2 BKAG und entsprechenden Definitionen der meisten anderen Bundesländer – durch eine Bezugnahme auf in § 129a Absatz 1 und 2 StGB genannte Straftaten, zu denen jeweils bestimmte prägende Zielsetzungen und Gefährdungsmomente hinzutreten müssen. Diese sind wiederum im Wesentlichen durch die Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung pp. (ABl. EU 2017 Nr. L 88, 6) vorgegeben.
Von der Bezugnahme auf § 129a Absatz 2 StGB ausgenommen bleiben allerdings die in § 129 Absatz 2 Nummer 4 und 5 StGB genannten Straftatbestände des Kriegswaffenkontrollgesetzes und des Waffengesetzes. Denn diese Strafbestände erfassen den Um-

gang mit Waffen und Kampfstoffen (wie das Herstellen, das Handel-Treiben, den Erwerb et cetera) im Vorfeld von Gefahren für Rechtsgüter. Demgegenüber handelt es sich bei den in § 129a Absatz 1 und Absatz 2 Nummer 1 bis 3 StGB genannten Tatbeständen um Verletzungs- und Gefährdungsdelikte, die besondere wichtige Rechtsgüter im Sinne der Rechtsprechung des BVerfG schützen (zu diesem Begriff: BVerfG, Urt. v. 16. Feb. 2023, 1 BvR 1547/19 = BVerfGE 165, 363 Rn. 105 m. w. N.).

**b. Zu § 201c Absatz 2 und 3 LVwG-Entwurf:**

Für die weiteren im Wesentlichen auf die Durchführung der elektronischen Aufenthaltsüberwachung bezogenen Regelungen kann im Fall einer elektronischen Aufenthaltsüberwachung nach § 201c LVwG-Entwurf auf die Parallelvorschriften des § 201b LVwG-Entwurf verwiesen werden. Soweit sich in Bezug auf die Weiterverarbeitung der erhobenen Daten bei einer elektronischen Aufenthaltsüberwachung zur Abwehr terroristischer Gefahrenlagen Spezifika ergeben, enthält § 201c Absatz 2 Satz 3 LVwG-Entwurf demgegenüber besondere Vorschriften. Für den Straftatbestand in § 201c Absatz 3 LVwG-Entwurf ist eine selbständige Normierung mit Blick auf die erhöhten Bestimmheitsanforderungen (Artikel 103 Absatz 2 GG) angezeigt.

**15. Zu Nummer 15 (Einführung von § 201d LVwG):**

Zukünftig wird in § 201d LVwG-Entwurf das Verfahren zur Anordnung der elektronischen Aufenthaltsüberwachung (in Teilen: neu) geregelt.

Bisher gilt für das Anordnungsverfahren § 186 Absatz 6 LVwG entsprechend. Die dortigen Regelungen sind jedoch auf verdeckte Maßnahmen gemäß § 185 bis 185c LVwG zugeschnitten, die ohne Wissen des Störers durchgeführt werden und die auf die offen durchgeführte elektronische Aufenthaltsüberwachung teilweise nicht ohne Friktionen übertragbar sind. Das gilt insbesondere für die Regelungen zum Gewährung rechtlichen Gehörs, soweit bei verdeckten Maßnahmen die vorherige Anhörung in der Regel deren Zweck vereiteln würde und diese Art von Maßnahmen grundsätzlich erst im Rahmen einer nachträglichen Benachrichtigung bekannt gemacht werden.

Gegen den Anordnungsbeschluss ist die Beschwere statthaft. Beschwerdeberechtigt sind die betroffene Person (§ 59 Absatz 1 FamFG) und – soweit der Antrag zurückgewiesen wird – als Antragsteller das Landeskriminal- oder Landespolizeiamt oder eine Polizeidirektion (§ 59 Absatz 2 FamFG). Die Beschwerdeberechtigung der antragstellenden Polizeibehörden bedarf keiner ausdrücklichen Erwägung im Gesetz.

**a. Zu § 201d Absatz 1 LVwG-Entwurf:**

§ 201d Absatz 1 LVwG-Entwurf stellt beide Formen der elektronischen Aufenthaltsüberwachung zunächst unverändert unter Richtervorbehalt. Für das Anordnungsverfahren gelten wie bisher die Vorschriften des Buches 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) ent-

sprechend. Für den Verfahrensablauf sehen allerdings die Absätze 2 bis 5 des § 201d LVwG-Entwurf in bestimmten Punkten Modifikationen vor.
Zeitlich ist die elektronische Aufenthaltsüberwachung weiterhin auf höchstens drei Monate befristet und kann einmal oder mehrfach um jeweils wiederum höchstens drei Monate verlängert werden, wenn die Anordnungsvoraussetzungen fortbestehen.

**b. Zu § 201d Absatz 2 und 3 LVwG-Entwurf:**

§ 201d Absatz 2 und 3 LVwG-Entwurf regeln die Anhörung der zu überwachenden Person insgesamt neu:

§ 201d Absatz 2 Satz 1 LVwG-Entwurf begründet zunächst die Pflicht zur persönlichen Anhörung der Person, deren Aufenthaltsort elektronisch überwacht werden soll, und zwar unabhängig davon, ob sich diese Pflicht bereits aus der allgemeinen Vorschrift des § 34 Absatz 1 Nummer 1 FamFG ergeben würde. Angesichts der Schwere des Grundrechtseingriffs ist es grundsätzlich angezeigt, dass das Gericht die zu überwachende Person persönlich anhört und sich dadurch einen persönlichen Eindruck verschafft.

§ 201d Absatz 2 Satz 2 LVwG-Entwurf ermöglicht – abweichend von § 33 Absatz 3 FamFG – dem Gericht die sofortige Vorführung der zu überwachenden Person anzuordnen, wenn diese nicht zum Anhörungstermin erscheint. Hiermit soll eine schnelle Entscheidung des Gerichts ermöglicht und einem missbräuchlichen Verhalten der zu überwachenden Person (mit dem Ziel, das Verfahren in die Länge zu ziehen) vorgebeugt werden. Ob eine ausreichende Entschuldigung vorliegt oder aus anderen Gründen von einer sofortigen Vorführung abgesehen werden kann, entscheidet das Gericht nach pflichtgemäßem Ermessen.

§ 201d Absatz 3 Satz 1 LVwG-Entwurf regelt, wann im Verfahren der einstweiligen Anordnung von der persönlichen Anhörung vor Anordnung der elektronischen Aufenthaltsüberwachung abgesehen werden kann. Angesichts der Eingriffstiefe ist dies nur bei zwingenden aus der Gefahrenlage herrührenden Gründen möglich. Allerdings hat bereits die bisherige (kurze) Praxis seit Inkrafttreten des § 201c LVwG am 15. April 2025 gezeigt, dass die Anhörung die zu überwachenden Person dazu verleiten kann, auf die gefährdete Person und dieser nahestehende Personen einzuwirken oder sie zur Zurücknahme der Zustimmungserklärung nach § 201b Absatz 3 LVwG-Entwurf zu drängen. Daher lässt § 201d Absatz 3 Satz 1 LVwG-Entwurf ein Absehen von der Anhörung bei Gefahr im Verzug zu. Gefahr im Verzug liegt zum einen vor, wenn angesichts der Gefahrenlage eine schnelles Einschreiten erforderlich ist. Gefahr im Verzug ist zum anderen aber insbesondere dann anzunehmen, wenn zu befürchten ist, dass bei Kenntnis der zu überwachenden Person vom Verfahrensgegenstand und der drohenden Überwachung bis zum Zeitpunkt des Termins einer persönlichen Anhörung eine Erhöhung der Gefahrenlage für die gefährdete Person eintritt.

Hat eine persönliche Anhörung vor Anordnung der elektronischen Aufenthaltsüberwachung gemäß § 201d Absatz 3 Satz 1 LVwG-Entwurf zu unterbleiben, ist diese gemäß § 201d Absatz 3 Satz 2 LVwG-Entwurf unverzüglich nachzuholen.

### c. Zu § 201d Absatz 4 LVwG-Entwurf:

§ 201d Absatz 4 LVwG-Entwurf übernimmt die bisher in § 201b Absatz 8 Satz 2 und 3 LVwG und § 201c Absatz 3 Satz 3 LVwG enthalten Regelungen.

### d. Zu § 201d Absatz 5 LVwG-Entwurf:

§ 201d Absatz 5 LVwG trifft für die Vollstreckung einer Anordnung der elektronischen Aufenthaltsüberwachung Regelungen:

Grundsätzlich wird der Anordnungsbeschluss mit Bekanntgabe wirksam (§ 40 Absatz 1 FamFG) und vollstreckbar (§ 86 Absatz 2 FamFG). Gemäß § 87 Absatz 2 FamFG darf die Vollstreckung aus ihm grundsätzlich (vergleiche aber § 53 Absatz 2 FamFG im Fall einer einstweiligen Anordnung) indes erst dann beginnen, wenn der Beschluss zugestellt ist oder gleichzeitig zugestellt wird. Um eine zügige Einleitung der Vollstreckung zu ermöglichen, soll gemäß § 201d Absatz 5 Satz 1 LVwG-Entwurf in der Regel die Polizei – entsprechend § 15 Absatz 2 Satz 1 FamFG, § 168 Absatz 2 Alternative 2 der Zivilprozessordnung – mit der Zustellung beauftragt werden.
Dies ermöglicht, zeitgleich mit der Zustellung die Vollstreckung einzuleiten. Denn die Polizei ist, wie § 201d Absatz 5 Satz 2 LVwG klarstellt, auf Grundlage von § 245 LVwG auch für die Vollstreckung zuständig und zwar nach Maßgabe der Bestimmungen über die Erzwingung von Handlungen, Duldungen oder Unterlassungen nach dem LVwG. Das heißt, dass zur Vollziehung der Anordnung durch die Polizei Zwangsgeld oder – sollte dieses als Vollzugsmittel erfolglos geblieben oder untunlich sein – unmittelbarer Zwang angewendet werden können.
Kein Mittel des Anordnungsvollzugs, sondern der Gefahrenabwehr ist die Ingewahrsamnahme der zu überwachenden Person gemäß § 204 Absatz 1 Nummer 5 Buchstabe b LVwG-Entwurf, wenn diese der Anordnung der elektronischen Aufenthaltsüberwachung nicht Folge leistet.

## 16. Zu Nummer 16 (Änderung von § 204 LVwG):

§ 204 LVwG-Entwurf gestaltet den Rechtsrahmen des Polizeigewahrsam neu. Im Mittelpunkt stehen die Gewahrsamstatbestände gemäß § 204 Absatz 1 Nummer 2 und 3 LVwG-Entwurf (vergleiche Allgemeiner Teil Punkt IV.).

### a. Zu § 204 Absatz 1 Satz 1 LVwG-Entwurf:

Die Anordnungskompetenz wird klar bei der Polizei verortet. Die Regelung korrespondiert mit der Regelung in § 204 Absatz 4 LVwG-Entwurf, die für die Ordnungsbehörden respektive deren Vollzugspersonal (kommunaler Ordnungsdienst) nur ein kurzfristiges Festhalterecht vorsieht.

### b. Zu § 204 Absatz 1 Nummer 2 LVwG-Entwurf:

Der Gewahrsamstatbestand des § 204 Absatz 1 Nummer 2 LVwG bleibt im Wesentlichen unverändert. Er erfasst aktuell Fälle, in denen die Ingewahrsamnahme einer Person zur Unterbindung einer „unmittelbar bevorstehende[n] Begehung oder Fortsetzung einer Straftat oder einer Ordnungswidrigkeit von erheblicher Bedeutung für die Allgemeinheit“ unerlässlich ist. Es ist geklärt, dass sich die einschränkende Formulierung „von erheblicher Bedeutung für die Allgemeinheit“ im Tatbestand des § 204 Absatz 1 Nummer 2 LVwG nur auf die Unterbindung von Ordnungswidrigkeiten bezieht (Schleswig-Holsteinisches OLG, Beschl. v. 28. April 2003, 2 W 207/02 = BeckRS 2003, 30316745; Martens in PdK SH A-15, LVwG § 204 Anm. 4.1). Dies wird durch die mit diesem Gesetzentwurf umgesetzte Umkehrung der Tatbestandsmerkmale („einer Ordnungswidrigkeit von erheblicher Bedeutung für die Allgemeinheit“ an erster und „einer Straftat“ an zweiter Stelle) klargestellt. Das Gewicht einer zu unterbindenden Straftat resp. die Straferwartung sind im Einzelfall im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigen.

Ergänzt wird der Tatbestand des § 204 Absatz 1 Nummer 2 LVwG um eine sogenannte legislative Prognosehilfe, die die erforderliche Prognose erleichtert, indem einige typische Anhaltspunkte angeführt werden, bei deren Vorliegen nach der Lebenserfahrung mit Straftaten oder mit Ordnungswidrigkeiten von erheblicher Bedeutung für die Allgemeinheit zu rechnen ist. Es handelt sich insoweit um Auslegungshilfen, die den Grundtatbestand unverändert lassen. Sie stellen mithin *keine* Regelbeispiele dar, die die Polizei oder den Richter binden oder eine Umkehr der Beweislast bewirken könnten (s. dazu BayVerfGH, Entscheidung v. 2. Aug. 1990, Vf.-VII-89 pp. = NVwZ 1991, 664, 667). Der Nutzen der legislativen Prognosehilfe besteht darin, polizeiliche Maßnahmen möglichst zu vereinheitlichen und ihre Messbarkeit und Vorhersehbarkeit zu erhöhen (Schmidbauer, 6. Aufl. 2023, PAG Art. 17 Rn. 48) und zugleich der Prognose eine erhöhte Legitimität zu verschaffen (BeckOK PolR Bayern/Grünewald, 24. Ed. 1.3.2024, PAG Art. 17 Rn. 45).

### c. Zu § 204 Absatz 1 Nummer 2 Buchstabe a LVwG-Entwurf:

Das erste Prognosekriterium (§ 204 Absatz 1 Nummer 2 Buchstabe a LVwG-Entwurf) ist ein nach außen manifestiertes Tatbekenntnis.
Insoweit kann die Ingewahrsamnahme insbesondere bei Personen gerechtfertigt sein, die eine Tat ankündigen. Dabei muss die angekündigte Tat hinreichend konkret beschrieben und auf einen nicht erst in ferner Zukunft liegenden Zeitpunkt bezogen sein. Diffuse Drohungen ohne Angaben zu Zeit und Ort rechtfertigen die Prognose einer unmittelbar bevorstehenden Tat nicht (s. BeckOK PolR Bayern a. a. O. Rn. 48). Ankündigung meint zudem eine Kundgabe gegenüber Dritten oder der Allgemeinheit.
Neben der Tatankündigung steht die Aufforderung zur Tat. Darunter ist – wie bei § 111 StGB (Öffentliche Aufforderung zu Straftaten) – eine über das bloße Befürworten hinausgehende Äußerung zu verstehen, die erkennbar von einer unbestimmten Personenmehrheit oder einer Person aus dem angesprochenen Personenkreis ein bestimmtes strafbares oder bußgeldbewehrtes Tun oder Unterlassen verlangt (vergleiche Heger in Lackner/Kühl, 30. Aufl. 2023, StGB § 111 Rn. 3 m. w. N.).
Der Ankündigung von oder Aufforderung zu einer Straftat oder Ordnungswidrigkeit von erheblicher Bedeutung für die Allgemeinheit gleichgestellt ist das Mitführen von Schriften

oder anderen Verkörperungen, die eine solche Ankündigung oder Aufforderung enthalten. Handelt es sich um entsprechende Ankündigungen oder Aufforderungen einer anderen Person als der, die in Gewahrsam genommenen wird, ist in der Regel zusätzlich zu verlangen, dass aus tatsächlichen Umständen abgeleitet werden kann, dass die in Gewahrsam genommene Person sich die schriftliche Ankündigung oder Aufforderung zu eigen macht.

**d. Zu § 204 Absatz 1 Nummer 2 Buchstabe b LVwG-Entwurf:**

Das zweite Prognosekriterium (§ 204 Absatz 1 Nummer 2 Buchstabe b LVwG-Entwurf) knüpft daran an, dass bei einer in Gewahrsam zu nehmenden Person selbst oder ihren Begleitpersonen bestimmte Gegenstände gefunden werden und Tatsachen die Annahme rechtfertigen, dass diese Gegenstände zur Begehung der Straftat oder Ordnungswidrigkeit bestimmt sind.
„Waffe“ ist bei § 204 Absatz 1 Nummer 2 Buchstabe b LVwG-Entwurf im umfassenden Sinne zu verstehen, das heißt nicht auf Waffen im Sinne des Waffenrechts beschränkt. Mithin sind ungeachtet ihrer waffenrechtlichen Einordnung etwa Messer, Totschläger, Schlagringe erfasst. Unter „Werkzeuge“ sind zum Beispiel typische Aufbruchinstrumente wie Bolzenschneider, Sägen, Glasschneider und ähnliche Gegenstände zu subsumieren. Der Begriff „sonstige Gegenstände“ stellt einen Auffangtatbestand dar. Es handelt sich um Gegenständen, die nicht per se auf Gewalthandlungen hindeuten, die jedoch als Angriffsmittel missbraucht werden können, sodass das Mitführen eines solchen Gegenstandes in einem entsprechenden Kontext ein Indiz für eine Tathandlung sein kann. Auch das Mitführen sogenannter Schutzwaffen kann die Prognose einer bevorstehenden Begehung von Straftaten oder erheblicher Ordnungswidrigkeiten im Einzelfall rechtfertigen.
Das bloße Auffinden der einschlägigen Gegenstände erfüllt das Prognosekriterium für sich noch nicht. Vielmehr bedarf es stets bestimmter Tatsachen, die im Einzelfall die Annahme begründen, dass die aufgefundenen Gegenstände zur Tatbegehung bestimmt sind (s. auch Schmidbauer a. a. O. Rn. 56). Außerdem ist zu beachten, dass selbst dann, wenn die Voraussetzungen des § 204 Absatz 1 Nummer 2 Buchstabe b LVwG-Entwurf erfüllt sind, im Rahmen der Verhältnismäßigkeit geprüft werden muss, ob nicht eine Sicherstellung der Gegenstände zur Gefahrenabwehr ausreichen kann. Dabei spielt eine entscheidende Rolle, ob und wie schnell die Gegenstände neu beschafft oder durch andere ersetzt werden können.
Die Prognose einer bevorstehenden Tatbegehung ist nicht nur in Bezug auf die Person gerechtfertigt, bei der die Gegenstände aufgefunden werden, sondern auch in Bezug auf Begleitpersonen. Dies setzt aber voraus, dass die in Gewahrsam genommene Person Kenntnis davon hat, dass ihre Begleitperson solche Gegenstände mitführt, respektive, dass ihre Kenntnis aufgrund bestimmter Tatsachen geschlossen werden kann. Dies erfordert eine sorgfältige Prüfung (BayVerfGH, a. a. O. = NVwZ 1991, 664, 667). Um eine Person als „Begleitperson“ der in Gewahrsam genommenen Person einzustufen, müssen beide Personen objektiv als zusammengehörig betrachtet werden können, etwa, weil beide Teil einer Gruppe sind und der Betroffene den Gegenständen daher so nah ist, dass auch er gegebenenfalls davon Gebrauch machen kann (s. BeckOK PolR Bayern a. a. O. Rn. 53).

### e. Zu § 204 Absatz 1 Nummer 2 Buchstabe c LVwG-Entwurf:

Auch das dritte Prognosekriterien – die Wiederholungsgefahr (§ 204 Absatz 1 Nummer 2 Buchstabe c LVwG-Entwurf) – begründet keine gesetzliche Vermutung. Vielmehr muss hier konkret feststellbar sein, dass die Begehung von Taten unmittelbar bevorsteht und der Gewahrsam unerlässlich ist. Grundlage können Registerauskünfte, polizeiliche Datenbanken, aber auch aus der Erfahrung früherer Einsätze der handelnden Polizeibeamten gewonnene Erkenntnisse sein (Schmidbauer a. a. O. Rn. 63). Ob mit einer unmittelbar bevorstehenden Tatbegehung „zu rechnen“ ist, bemisst sich nach den zeitlichen und örtlichen Umständen im Einzelfall. Aus der Formulierung „in der Vergangenheit mehrfach“ folgt, dass der Betroffene mindestens bei zwei Gelegenheiten in der Vergangenheit negativ aufgefallen sein muss. Die Einschränkung „weitere gleichartige Taten“ bedeutet, dass zwischen den Taten in der Vergangenheit und der gegebenenfalls zu verhindernden Tat eine qualitative Vergleichbarkeit besteht.

### f. Zu § 204 Absatz 1 Nummer 3 LVwG-Entwurf:

§ 204 Absatz 1 Nummer 3 LVwG-Entwurf enthält einen neuen Gewahrsamstatbestand. Er ist primär als Auffangtatbestand konzipiert (vergleiche Allgemeiner Teil Punkt IV.2.).

§ 204 Absatz 1 Nummer 3 LVwG-Entwurf erfordert – anders als § 204 Absatz 1 Nummer 2 LVwG-Entwurf – keine gegenwärtige Gefahr. Ausreichend ist eine konkrete Gefahr. Das Absenken der Eingriffsschwelle wird kompensiert, indem nur besonders gewichtige Rechtsgüter im Sinne der Rechtsprechung des BVerfG geschützt sind (vergleiche: BVerfG, Urt. v. 16. Feb. 2023, 1 BvR 1547/19 = BVerfGE 165, 363 Rn. 105 m. w. N.).
Eine konkrete Gefahr bezeichnet eine Sachlage, die nach allgemeiner Lebenserfahrung bei ungehindertem Verlauf des objektiv zu erwartenden Geschehens im Einzelfall mit hinreichender Wahrscheinlichkeit zu einer Verletzung eines Rechtsguts führt. An die durch die Polizei in diesen Zusammenhängen zu treffende Gefahrenprognose sind wegen des Eingriffs in die Freiheit der Person hohe Anforderungen zu stellen. Dies gilt insbesondere mit Blick auf die einschlägige Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte in Bezug auf Artikel 5 Absatz 1 Satz 2 Buchstabe c Alternative 2 EMRK. Die Ingewahrsamnahme ist insofern nur zur Verhinderung einer – insbesondere nach Ort, Zeit und Opfern – konkreten und bestimmten Handlung möglich (EGMR, Urt. v. 22. Oktober 2018, 35553/12 pp. = NVwZ 2019, 135 Rn. 89 f.).

Sehr wichtig zu sehen ist, dass dem Tatbestandsmerkmal unerlässlich besondere Bedeutung zukommt. (s. auch Schmidbauer, 6. Aufl. 2023, PAG Art. 17 Rn. 68 f.). So dürfen erstens andere Maßnahmen – namentlich Observationen, verdeckte technische Mittel, Aufenthaltsanordnungen und elektronische Aufenthaltsüberwachung – nicht zur Gefahrenabwehr ausreichen. Zweitens muss feststehen, dass die Störerin oder der Störer sich an bestimmte konkrete Verbote und Gebote nicht gehalten hat oder zum Ausdruck gebracht hat, dass er sich an sie nicht halten wird. Schließlich müssen das durch die polizeiliche Maßnahme zu schützende Rechtsgut und das mit hohem Verfassungsrang geschützte Rechtsgut der Freiheit der Person, in das eingegriffen wird, in einem angemessenen Verhältnis zueinander stehen.

### g. Zu § 204 Absatz 1 Nummer 5 LVwG-Entwurf:

Die bisherigen Gewahrsamstatbestände in § 204 Absatz 1 Nummern 4, 5 und 6 LVwG werden zusammengeführt.

### h. Zu § 204 Absatz 2 LVwG-Entwurf:

Der Gewahrsamstatbestand gemäß § 204 Absatz 2 LVwG wird unverändert fortgeführt.

### i. Zu § 204 Absatz 3 LVwG-Entwurf:

Der Regelungsgehalt des Gewahrsamstatbestandes gemäß § 204 Absatz 3 LVwG wird fortgeführt. Die Ersetzung der bisher aufgelisteten Einzelfälle durch die Wörter „gerichtlich angeordnete Freiheitsentziehung“ und der aufgezählten Anstalten und Einrichtungen durch das Wort „Vollzugseinrichtung“ schafft eine größere sprachliche Klarheit und Prägnanz der Vorschrift und gewährleistet eine Einbeziehung aller von Telos erfassten Sachverhalte.

### j. Zu § 204 Absatz 4 LVwG-Entwurf:

In der Praxis besteht ein Bedürfnis, dass Vollzugskräfte der Ordnungsbehörden respektive Mitarbeiter des sogenannten kommunalen Ordnungsdienstes bei Vorliegen der Voraussetzungen für eine Ingewahrsamnahme in bestimmten Fällen zum Beispiel eine hilflose Person oder einen Störer, der des Platzes verwiesen werden soll, bis zum Eintreffen der Polizei festhalten dürfen. Eine solche Festhaltebefugnis fehlt im LVwG. Diese Lücke schließt der neue § 204 Absatz 4 LVwG-Entwurf.

### k. Zu § 204 Absatz 5 LVwG-Entwurf:

Die Regelung entspricht im Wesentlichen dem bisherigen Regelungsgehalt des § 204 Absatz 5 LVwG. Neu aufgenommen ist lediglich § 204 Absatz 5 Nummer 2 LVwG-Entwurf. Sie dient der Klarstellung.

### l. Zu § 204 Absatz 6 LVwG-Entwurf:

Der neue § 204 Absatz 6 LVwG-Entwurf normiert erstmals für Schleswig-Holstein eine Höchstdauer des Gewahrsams.
Die Regelung über die Höchstdauer greift nur für Fälle, in denen der Gewahrsamsgrund nicht weggefallen ist, also nur bei noch fortdauernder Gefahrenlage.
Die Entscheidung über die Fortdauer beziehungsweise Länge des Gewahrsams ist nach Maßgabe von Artikel 104 Absatz 2 GG der Entscheidung einer Richterin oder eines Richters überantwortet. Sie ist im Einzelfall nach Verhältnismäßigkeitsgesichtspunkten festzulegen und kann im Rahmen der maximal zulässigen Gesamtdauer von 2 Monaten variabel, das heißt auch mehrfach mit jeweils kürzerer Dauer verlängert werden. Die Höchstdauer von zwei Monaten darf keinesfalls überschritten werden.
Der Eingriff in die Freiheit der Person ist nur solange hinzunehmen, als der legitime Schutzanspruch der staatlichen Gemeinschaft nicht anders gesichert werden kann als

durch Inhaftierung. Mit zunehmender Gewahrsamsdauer vergrößert sich regelmäßig das Gewicht des Freiheitsanspruchs gegenüber dem Interesse der Allgemeinheit an einer wirksamen Gefahrenprävention. Das heißt, je länger ein präventiv-polizeilicher Gewahrsam dauert, desto strenger sind deshalb die Voraussetzungen für die Verhältnismäßigkeit des Freiheitsentzugs. Dabei ist neben dem unumkehrbaren Entzug der körperlichen Bewegungsfreiheit auch die Beeinträchtigung anderer Grundrechte in Rechnung zu stellen. Hierzu zählen insbesondere auch eine anzunehmende psychische Belastung sowie potentiell negative Auswirkungen auf das soziale Umfeld.

Die jetzt normierte Höchstdauer des durch richterliche Entscheidung angeordneten Präventivgewahrsams ist nach Maßgabe der obergerichtlichen Rechtsprechung mit dem Grundrecht der Freiheit der Person und dem Rechtsstaatsprinzip vereinbar.

## 17. Zu Nummer 17 (Änderung von § 205 LVwG):

Die bisherige Regelungen des § 205 LVwG „Verfahren bei amtlichen Gewahrsam“ wird insgesamt neu gestaltet und erhält eine neue Überschrift („Behandlung in Gewahrsam genommener Personen“).

### a. Zu § 205 Absatz 1 LVwG-Entwurf:

§ 205 Absatz 1 LVwG enthält bisher eine (Klammer-)Definition des „amtlichen Gewahrsams“, an den die verfahrensbezogenen Regelung des § 205 LVwG anknüpfen (also bestimmte Belehrungen, die Unterrichtung nahestehender Personen, die abgesonderte Unterbringung und Maßnahmen zur Aufrechterhaltung der Ordnung im „amtlichen Gewahrsam“). Der Begriff des „amtlichen Gewahrsams“ war mit dem LVwG eingeführt worden und sollte als Oberbegriff alle Fälle der Freiheitsentziehung im Verwaltungswege erfassen unabhängig davon, ob die Rechtsvorschrift, auf die sich die Freiheitsentziehung stützte, von Gewahrsam, Verwahrung, Haft oder Unterbringung sprach (Martens in PdK SH A-15, LVwG 205 Anm. 1). Es ging mithin darum, für alle Formen der Freiheitsentziehung durch Polizei und Ordnungsbehörden einheitliche Regelungen zur Behandlung der betroffenen Person aufzustellen. Da mittlerweile jedoch für die (historisch betrachtet) miterfassten Freiheitsentziehungen nach § 127 StPO, dem Ausländerrecht oder dem PsychHG (vergleiche Martens a. a. O.) speziellere Regelungsregime zum Umgang mit den betroffenen Personen, denen die Freiheit entzogen wird, geschaffen sind, bedarf es eines solchen verschiedene Rechtsbereiche übergreifenden Regelungsregimes nicht mehr. Aus diesem Grund wird die Vorschrift des § 205 LVwG auf den Vollzug des Polizeigewahrsams nach § 204 LVwG ausgerichtet, wobei die diesbezüglichen Regelungen insgesamt überarbeitet und ausgebaut werden.

Die ursprüngliche Zielrichtung des § 205 LVwG, für alle Formen des Freiheitsentziehung übergreifende Regelungen zum Umgang mit der betroffenen Person aufzustellen, hat allerdings noch dort eine Berechtigung, wo Personen, denen aufgrund anderer Vorschriften als § 204 LVwG die Freiheit entzogen wird, vorübergehend in der Obhut der Polizei befinden (zum Beispiel nach einer Verhaftung im Vorwege einer Vorführung), soweit gegenüber § 205 LVwG-Entwurf speziellere Vorschriften zur Behandlung der betroffenen

Person (wie zum Beispiel §§ 114a ff. StPO) fehlen. Für diese Fallkonstellation erklärt zukünftig § 205 Absatz 7 LVwG-Entwurf die Vorschriften über Behandlung von Polizeigewahrsam befindlichen Personen gemäß § 205 LVwG-Entwurf für entsprechend anwendbar.

**b. Zu § 205 Absatz 2 LVwG-Entwurf:**

Der bisher durch Verweis auf § 200 Absatz 2 LVwG (Verfahren bei der Vorführung) in Bezug genommene Regelungsinhalt wird zur Erhöhung der Normenklarheit übernommen.

**c. Zu § 205 Absatz 3 LVwG-Entwurf:**

Der Regelungsgehalt des bisherigen § 205 Absatz 3 LVwG wird im Wesentlichen übernommen. Ergänzt wird das Gebot, minderjährige und erwachsene Personen getrennt unterzubringen. Neu ist, dass bei der Entscheidung über die Unterbringung die Persönlichkeit, die Bedürfnisse und der Wille von trans-, intergeschlechtlichen sowie nicht-binären Personen grundsätzlich zu berücksichtigen sind („Soll-Vorschrift“). Besteht jedoch eine Gefährdung von Sicherheit und Ordnung, kann eine abweichende Unterbringungsform angeordnet werden.

**d. Zu § 205 Absatz 4 LVwG-Entwurf:**

Personen, die infolge einer psychischen Störung ihr Leben, ihre Gesundheit oder bedeutende Rechtsgüter anderer erheblich gefährden, sind grundsätzlich nach dem speziellen Gefahrenabwehrrecht des PsychHG unterzubringen. Gleichwohl kann sich auch im Rahmen einer allgemeinen gefahrenabwehrrechtlichen Ingewahrsamnahme zeigen, dass gesundheitliche, psychische oder soziale Faktoren die Gefahrenlage hergerufen oder verstärkt haben. In diesem Fall soll bei einer längerfristigen Freiheitsentziehung sichergestellt werden, dass die festgehaltene Person Unterstützungsmaßnahmen erhält, die geeignet sind, die Wirksamkeit der kritischen Faktoren zu reduzieren, mit dem Ziel der Gefahrenlage für die Zukunft vorzubeugen. In Betracht kommen insbesondere die Einrichtung einer rechtlichen Betreuung, psychiatrische und psychologische Anbindung, Anti-Gewalt-Training, Gewaltpräventionsambulanzen, Drogenhilfeeinrichtungen. Die Präventionsmaßnahmen werden regelmäßig während des Gewahrsams lediglich eingeleitet werden können und müssen daher nach der Beendigung der Freiheitsentziehung fortgesetzt werden.

**e. Zu § 205 Absatz 5 LVwG-Entwurf:**

§ 205 Absatz 5 Satz 1 LVwG-Entwurf übernimmt den bisherigen Regelungsgehalt von § 205 Absatz 4 LVwG.

**f. Zu § 205 Absatz 6 LVwG-Entwurf:**

§ 205 Absatz 6 Satz 1 LVwG-Entwurf führt die aktuell in § 204 Absatz 4 Satz 2 LVwG enthaltene Rechtsgrundlage zur Beobachtung der festgehaltenen Person mittels offener Bildübertragung fort.

§ 205 Absatz 6 Satz 2 bis 6 LVwG-Entwurf gestatten darüber hinaus in engen Grenzen auch Bildaufzeichnungen offen anzufertigen: Zielrichtung ist gleichermaßen eine Hemmschwelle für Übergriffe auf Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte zu schaffen, als auch das Handeln der Aufsichtspersonen transparent zu dokumentieren. Vor diesem Hintergrund dürfen Aufzeichnungen grundsätzlich nur dann angefertigt werden, wenn Polizeivollzugsbeamtinnen oder Polizeivollzugsbeamte im Gewahrsamsraum anwesend sind. In anderen Situationen – ohne Anwesenheit von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten – sind grundsätzlich Bildaufnahmen nur kurzzeitig (für einen Zeitraum von einigen Sekunden) zulässig, wenn eine Gefahr für Leib oder Leben der Person zu besorgen ist, insbesondere Suizidgefahr besteht.

Durch den Verweis in § 205 Absatz 6 Satz 7 LVwG-Entwurf auf § 184a Absatz 6 und 7 LVwG gelten die Aufbewahrungs- und Löschfristen für Aufzeichnungen körpernah getragener Aufzeichnungsgeräte (sogenannter Body-Cams) entsprechend.

Die Bundesstelle zur Verhütung von Folter kommt in ihrem Jahresbericht 2016 zu dem Schluss, dass der Einsatz von Video- und Tonüberwachung in Gewahrsamsräumen sich positiv zum Schutz aller involvierten Personen auswirkt.

**g. Zu § 205 Absatz 7 LVwG-Entwurf:**

Die Regelungen des § 205 Absatz 1 bis 6 LVwG-Entwurf gelten unmittelbar zukünftig nur noch für den Polizeigewahrsam gemäß § 204 LVwG. Zu den Hintergründen dieser Neuregelung ist auf die Begründung zu § 205 Absatz 1 LVwG-Entwurf zu verweisen. In Fällen, in denen sich Personen, denen aufgrund anderer Vorschriften als § 204 LVwG die Freiheit entzogen wird, vorübergehend in der Obhut der Polizei befinden – zum Beispiel nach einer Verhaftung im Vorwege einer Vorführung – ist jedoch sachgerecht, die Vorschriften § 205 Absatz 1 bis 6 für die Behandlung der festgehaltenen Person entsprechend anzuwenden, wenn und soweit gegenüber § 205 LVwG-Entwurf speziellere Vorschriften (wie zum Beispiel §§ 114a ff. StPO) fehlen. Die Erstreckung des Anwendungsbereich auf die einschlägigen Fallkonstellationen gewährleistet die neue Vorschrift des § 205 Absatz 7 LVwG-Entwurf.

**h. Zu § 205 Absatz 8 LVwG-Entwurf:**

Gemäß § 205 Absatz 8 Satz 1 LVwG-Entwurf wird der längerfristige Polizeigewahrsam, soweit er im Wege der Amtshilfe in einer Justizvollzugsanstalt durchgeführt wird, nach den Regelungen der Zivilhaft vollzogen. Personen im längerfristigen Polizeigewahrsam haben dabei die Stellung eines Gefangenen in der Zivilhaft. Die Zivilhaft unterscheidet sich grundlegend von der Strafhaft, da sie keine Strafe darstellt, sondern der Durchsetzung oder Sicherung zivilrechtlicher beziehungsweise verwaltungsrechtlicher Verpflichtungen dient und zeitlich begrenzt ist. Der Vollzug des längerfristigen Polizeigewahrsams dient in diesem Zusammenhang der kurzfristigen Sicherstellung der öffentlichen Sicherheit. Diese Kurzfristigkeit prägt auch den Ablauf des Vollzuges. Resozialisierungsmaßnahmen, die im Strafvollzug eine schrittweise Wiedereingliederung in die Gesellschaft fördern, sind in der Zivilhaft nicht vorgesehen.

Gemäß § 171 Strafvollzugsgesetzes des Bundes (StVollzG) gelten § 119 Absatz 5 und 6 StPO sowie die Vorschriften über den Vollzug der Freiheitsstrafe (§§ 3 bis 49 StVollzG sowie §§ 51 bis 121b StVollzG) entsprechend, soweit nicht Eigenart und Zweck der Haft entgegenstehen oder im StVollzG (namentlich in §§ 171a bis 175 StVollzG sowie § 178 Absatz 2 Satz 1 StVollzG) etwas anderes bestimmt ist. Dementsprechend verweist § 171 StVollzG auch auf § 88 StVollzG (Besondere Sicherungsmaßnahmen) und § 91 StVollzG (Anordnung besonderer Sicherungsmaßnahmen), welche nahezu inhaltsgleich mit den Regelungen der §§ 108 und 109 des Landesstrafvollzugsgesetzes sind. Somit können Sicherungsmaßnahmen auf Grundlage des StVollzG gegenüber in Gewahrsam genommenen und in Justizvollzugsanstalten untergebrachten Personen angeordnet werden.

§ 205 Absatz 8 Satz 2 LVwG-Entwurf ermöglicht den notwendigen Informationsfluss von der Polizei an die Justizvollzuganstalt, in welcher der Polizeigewahrsam im Wege der Amtshilfe vollzogen wird.

**18. Zu Nummer 18 (Einführung von § 205a LVwG-Entwurf):**

Das Verfahren zur Herbeiführung der richterlichen Entscheidung über die Zulässigkeit und Fortdauer der Ingewahrsamnahme erhält mit § 205a LVwG-Entwurf eine selbständige, geschlossene und in wesentlichen Punkten neue Regelung.

**a. Zu § 205a Absatz 1 LVwG-Entwurf:**

Die Vorschrift übernimmt im Wesentlichen den Regelungsgehalt der aktuell in § 204 Absatz 6 LVwG enthaltenen Verweisung auf die Vorschrift des § 181 Absatz 5 LVwG aus dem Recht der Identitätsfeststellung.

**b. Zu § 205a Absatz 2 LVwG-Entwurf:**

Die Vorschrift bestimmt das örtlich zuständige Amtsgericht und das anzuwendende Verfahrensrecht, nämlich den Allgemeinen Teil (Buch 1) und den Abschnitt über das Verfahren bei Freiheitsentziehung (Buch 7) des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG).

**c. Zu § 205a Absatz 3 LVwG-Entwurf:**

Mit dem neuen Anspruch auf anwaltliche Vertretung nach § 205a Absatz 3 LVwG-Entwurf sieht das LVwG eine zusätzliche verfahrensrechtliche Absicherung der Rechte der betroffenen Person (neben den bestehenden Rechten: Belehrung, Gelegenheit zur Benachrichtigung, Überprüfung der Gewahrsamsvoraussetzungen durch eine Richterin oder einen Richter) vor.

**d. Zu § 205a Absatz 4 LVwG-Entwurf:**

Der neue § 205a Absatz 4 LVwG-Entwurf schafft einen Anspruch auf eine richterliche Überprüfung der Freiheitsentziehung, wenn keine gerichtliche Entscheidung über die Zulässigkeit der Freiheitsentziehung ergangen ist. Damit wird der Anspruch aus Artikel 19 Absatz 4 GG realisiert, unabhängig von den Voraussetzungen eines Fortsetzungsfeststellungsantrages in entsprechender Anwendung von § 113 Absatz 1 Satz 4 Verwaltungsgerichtsordnung.

**e. Zu § 205a Absatz 5 LVwG-Entwurf:**

Die Vorschrift regelt klarstellend die Kostentragung.

**19. Zu Nummer 19 (Änderung von § 258 LVwG):**

Die Änderung von § 258 Absatz 2 Nummer 4 LVwG ist redaktioneller Natur. Sie ist aufgrund der Aufgabe der Legaldefinition für den „amtlichen Gewahrsam“ in § 205 LVwG-Entwurf erforderlich. Denn anders als in jener Vorschrift wird der Begriff „amtlicher Gewahrsam“ bei § 258 Absatz 2 Nummer 4 und 5 LVwG als Oberbegriff für alle Fälle der Freiheitsentziehung – unabhängig davon, ob die Rechtsvorschrift, auf die sich die Freiheitsentziehung stützt, von Gewahrsam, Verwahrung, Haft oder Unterbringung spricht – auch in Zukunft benötigt. § 258 Absatz 2 Nummer 4 und 5 LVwG erlaubt den Schusswaffeneinsatz bei Flucht oder gewaltsamer Befreiung aus bestimmten Formen des amtlichen Gewahrsams im vorbezeichneten Sinne. Die vormals in § 205 LVwG verortete (Klammer-)Definition, an die die Vorschrift über den Schusswaffengebrauch schon bisher anknüpfte, wird in § 258 Absatz 2 Nummer 4 LVwG inhaltlich unverändert fortgeführt.

**II. Zu Artikel 2 (Inkrafttreten)**

Artikel 2 regelt das Inkrafttreten dieses Gesetzes.