Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften

Vorblatt

A. Zielsetzung

Das Gesetz verfolgt im Wesentlichen drei Ziele. Zunächst soll eine Rechtsgrundlage dafür geschaffen werden, bisher unverbundene Daten und Datenquellen des Polizeivollzugsdienstes in einer Analyseplattform zusammenzuführen, um die vorhandenen Datenbestände durch Suchfunktionen systematisch erschließen zu können (automatisierte Datenanalyse). Zudem soll eine Rechtsgrundlage zur Erhebung, Verarbeitung und Übermittlung von Standortdaten geschaffen werden, die nach Anwahl der Notrufnummer mittels eines mobilen Endgerätes automatisiert und ohne Interaktion der anrufenden Person generiert und übermittelt wurden. Dies ermöglicht dem Polizeivollzugsdienst unter Nutzung der sogenannten Advanced-Mobile-Location-Technologie (AML-Technologie) die schnelle Ortung einer hilfesuchenden Person. Schließlich sollen die Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst mit Befugnissen zur Entwicklung, zum Training, zum Testen, zur Validierung und zur Beobachtung von informationstechnischen Produkten ausgestattet werden, um die eigenständige Entwicklung von informationstechnischen Produkten zu ermöglichen und die Aabhängigkeit von ausländischen, insbesondere außereuropäischen Produkten zu verringern. Durch rechtliche, technische und organisatorische Maßgaben wird dabei ein hohes Schutzniveau für personenbezogene Daten gewährleistet und gleichzeitig die Entwicklung und Nutzung von diskriminierungsfreien informationstechnischen Produkten sichergestellt.

B. Wesentlicher Inhalt

Der Gesetzentwurf sieht im Wesentlichen die Schaffung von Rechtsgrundlagen zur Einführung einer automatisierten Datenanalyse, zur Erhebung, Verarbeitung und Übermittlung von Standortdaten, die nach Anwahl der Notrufnummer mittels eines mobilen Endgerätes automatisiert generiert und übermittelt wurden, sowie zur Verarbeitung von Daten bei der Entwicklung, dem Training, dem Testen, der Validierung und der Beobachtung von informationstechischen Produkten.

C. Alternativen

Keine.

D. Kosten für die öffentlichen Haushalte

Die Umsetzung der durch die Änderung des Polizeigesetzes geschaffenen Rechtsgrundlagen führt nach einer ersten Grobabschätzung zu Mehrausgaben für den Landeshaushalt in Höhe von jährlich rund 10 Millionen Euro. Es handelt sich dabei um Personal- und Sachmittel für die Beschaffung von Software und für den Betrieb der zum Teil komplexen informationstechnischen Infrastruktur. Diese Mehrausgaben sind bereits im Staatshaushaltsplan 2025 / 2026 im Bereich des Innenministeriums vollständig etatisiert. Hinsichtlich der Schaffung einer Rechtsgrundlage für die Verarbeitung von Daten bei der Entwicklung, dem Training, dem Testen, der Validierung und der Beobachtung von informationstechnischen Produkten außerhalb von rein wissenschaftlichen Forschungsarbeiten können der Polizei Kosten im Rahmen von Softwarebeschaffung, -entwicklung und -erprobung, die sich derzeit noch nicht beziffern lassen, entstehen. Die Deckung dieser Kosten erfolgt jedoch im Rahmen der vorhandenen Mittel der Polizei. Über eventuell zukünftig entstehende Mehrbedarfe entscheidet der Haushaltsgesetzgeber.

E. Bürokratievermeidung, Prüfung Vollzugstauglichkeit

Der Gesetzentwurf verursacht keine erheblichen Auswirkungen für Unternehmen, Verwaltung und Bürgerinnen und Bürger oder aufwendige Verwaltungsverfahren. Von der Durchführung eines Praxis-Checks und einer Bürokratielastenschätzung wurde daher abgesehen. Gleichwohl können punktuell Mehraufwände beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen seiner gesetzlichen Zuständigkeit entstehen, die im Rahmen vorhandener Mittel gedeckt werden.

F. Nachhaltigkeitscheck

Es ergeben sich positive Auswirkungen auf den Zielbereich IV. Wohl und Zufriedenheit.

G. Digitaltauglichkeits-Check

Die automatisierte Datenanalyse ermöglicht es dem Polizeivollzugsdienst, vorhandene Datenbestände durch Suchfunktionen systematisch zu erschließen. Dadurch werden Medienbrüche reduziert und manuelle Abfragen verschiedener

Datenquellen entbehrlich, die aufgrund großer Datenmengen aus unterschiedlichen Quellen sowie unterschiedlicher Dateiformate bislang zeitaufwendig und komplex sind. Durch Nutzung der AML-Technologie werden das Verfahren zur schnellen Standortbestimmung einer hilfesuchenden Person mittels einer Web-Anwendung digitalisiert und Medienbrüche reduziert. Zudem wird die Genauigkeit der Standortbestimmung durch die kombinierte Nutzung verschiedener technischer Positionsdienste erheblich verbessert. Durch die Einführung entsprechender elektronischer Fachverfahren ist daher sowohl bezogen auf die Analyse von polizeilichen Datenbeständen als auch bezogen auf die Standortbestimmung von notrufenden Personen eine Vereinfachung und Beschleunigung polizeilicher Abläufe zu erwarten.

H. Sonstige Kosten für Private

Keine.

Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften

Vom

Artikel 1
Änderung des Polizeigesetzes

Das Polizeigesetz vom 6. Oktober 2020 (GBl. S. 735, ber. S. 1092) wird wie folgt geändert:

1. Nach § 45 wird folgender § 45a eingefügt:

„§ 45a
Verarbeitung von Standortdaten bei Anwahl der Notrufnummer 110

(1) Das Präsidium Technik, Logistik, Service der Polizei kann die im Rahmen einer Notrufverbindung von einem mobilen Telekommunikationsendgerät generierten und automatisch übermittelten personenbezogenen Daten, einschließlich der Standortdaten, erheben, speichern und auf Abruf an die zuständigen Notrufabfragestellen übermitteln. Die Daten sind 60 Minuten nach deren Erhebung zu löschen. Eine Verarbeitung zu einem anderen Zweck als zur Übermittlung an die zuständigen Notrufabfragestellen ist unzulässig.

(2) Der Polizeivollzugsdienst kann als zuständige Notrufabfragestelle im Einzelfall die in Absatz 1 Satz 1 genannten Daten erheben, verarbeiten und speichern, soweit dies zur Abwehr einer Gefahr für Leib, Leben oder Freiheit erforderlich ist. Die Daten sind spätestens nach sechs Monaten zu löschen.“

2. Nach § 47 wird folgender § 47a eingefügt:

„§ 47a
Automatisierte Datenanalyse

(1) Der Polizeivollzugsdienst kann nach Maßgabe der Absätze 2 bis 7 in polizeilichen Dateisystemen gespeicherte personenbezogene Daten auf einer Analyseplattform automatisiert zusammenführen, verknüpfen, abgleichen, aufbereiten, auswerten und bewerten (automatisierte Datenanalyse), wenn

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

2. bestimmte Tatsachen die Annahme rechtfertigen, dass

   a) innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat von erheblicher Bedeutung begangen wird, die auch im Einzelfall schwer wiegt,

   b) die automatisierte Datenanalyse zur Verhütung dieser Straftat erforderlich ist und

   c) die Verwirklichung der Straftat zu einer Gefahr für das geschützte Rechtsgut führen würde,

   oder

3. bestimmte Tatsachen die Annahme rechtfertigen, dass besonders schwere Straftaten begangen werden sollen und die automatisierte Datenanalyse zur Verhütung dieser Straftaten erforderlich ist.

(2) Die automatisierte Datenanalyse unterstützt den Polizeivollzugsdienst bei der Erfüllung seiner Aufgaben, indem sie Informationen bereitstellt, die es dem Polizeivollzugsdienst ermöglichen, eigene Bewertungen, Prognosen und Entscheidungen zu treffen. Dabei ist sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Eine abschließende Bewertung der bereitgestellten Informationen und die Entscheidung über weitere Maßnahmen werden durch den Polizeivollzugsdienst getroffen. Die automatisierte Datenanalyse wird manuell ausgelöst und erfolgt anhand anlassbezogener und zielgerichteter Suchkriterien, die sich aus einem konkreten Sachverhalt bezogen auf einen Anlass im Sinne des Absatzes 1 ergeben. Bei Maßnahmen nach Absatz 1 Nummern 2 und 3 ist der Suchvorgang auf die in den §§ 6 und 7 genannten Personen auszurichten. Eine direkte Anbindung der Analyseplattform an Internetdienste ist unzulässig.

(3) Zum Zweck der automatisierten Datenanalyse können eigene Vorgangsdaten, Falldaten, Daten aus polizeilichen Auskunftssystemen und Daten aus dem

polizeilichen Informationsaustausch zusammengeführt werden. Verkehrsdaten, Daten aus Asservaten, Daten im Sinne des Satzes 1 aus gezielten Abfragen in landesfremden Datenbeständen, Daten in gesondert geführten staatlichen Registern sowie einzelne gesondert gespeicherte Daten aus Internetquellen können ergänzend einbezogen werden, soweit dies im Einzelfall erforderlich ist. Verkehrsdaten aus Funkzellenabfragen sowie Telekommunikationsdaten dürfen bei einer Maßnahme nach Absatz 1 Nummer 3 nicht in die Analyse einbezogen werden. Einzelfallbezogen auf der Analyseplattform gespeicherte Daten nach Satz 2 sind spätestens nach Ablauf von zwei Jahren zu löschen, soweit eine weitere Speicherung der Daten nicht erforderlich ist. Eine weitere Speicherung nach Satz 4 kann im Einzelfall höchstens zweimal durch eine schriftliche und begründete Anordnung der Leitung eines regionalen Polizeipräsidiums, des Polizeipräsidiums Einsatz oder des Landeskriminalamts um jeweils höchstens ein Jahr verlängert werden. Personenbezogene Daten, die aus einer Wohnraumüberwachung oder einer Online-Durchsuchung gewonnen wurden, dürfen nicht in die automatisierte Datenanalyse einbezogen werden.

(4) Technisch-organisatorische Vorkehrungen insbesondere zur Einhaltung der Zweckbindung nach § 15 Absätze 2 und 3 werden in einer Verwaltungsvorschrift geregelt, die in dem für den Geschäftsbereich des Innenministeriums vorgesehenen amtlichen Bekanntmachungsblatt zu veröffentlichen ist. Diese beinhaltet insbesondere

1. ein Rollen- und Rechtekonzept,

2. ein Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten,

3. ein Konzept zur Zugriffskontrolle, das auch verdachtsunabhängige Stichprobenkontrollen der Zugriffe vorsieht, sowie

4. nähere Bestimmungen über den Inhalt der erforderlichen Begründung nach Absatz 3 Satz 5 und Absatz 7 Satz 3.

Die Vorgaben in der Verwaltungsvorschrift dienen unter Berücksichtigung der in Absatz 1 beschriebenen Eingriffsschwellen dem übergeordneten Ziel, die Datenbestände auf das für den Analysezweck erforderliche Maß zu begrenzen und die Einbeziehung von Daten unbeteiligter Personen möglichst zu vermeiden.

(5) Das Rollen- und Rechtekonzept nach Absatz 4 Satz 2 Nummer 1 regelt die Verteilung sachlich eingeschränkter Zugriffsrechte. Die Zugriffsrechte sind nach dem Prinzip auszugestalten, dass die Zahl der Zugriffsberechtigten umso geringer ist, desto umfangreicher und sensibler die von der Zugriffsberechtigung umfassten Daten sind. Die dienstrechtliche Stellung der Zugriffsberechtigten, ihre Funktion und ihre spezifische Qualifizierung in Bezug auf den Umfang der jeweiligen Zugriffsrechte sind festzulegen.

(6) Das Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten nach Absatz 4 Satz 2 Nummer 2 legt fest, welche personenbezogenen Daten in welcher Weise in die automatisierte Datenanalyse einbezogen werden dürfen. Ausgangspunkt ist die Differenzierung nach einerseits verurteilten, beschuldigten, verdächtigen und sonstigen Anlasspersonen sowie deren Kontaktpersonen und andererseits unbeteiligten Personen. Zum Schutz unbeteiligter Personen werden deren personenbezogene Vorgangsdaten in eine automatisierte Datenanalyse nicht einbezogen. Hinsichtlich der Kategorisierung von Daten nach dem Gewicht des Grundrechtseingriffs bei der Datenerhebung müssen abstrakte Regelungen getroffen werden, die der eingeschränkten Verwendbarkeit von Daten aus schwerwiegenden Grundrechtseingriffen Rechnung tragen. Durch technisch-organisatorische Vorkehrungen muss sichergestellt werden, dass diese Regelungen praktisch wirksam werden.

(7) Eine Maßnahme nach Absatz 1 erfolgt auf Anordnung der Leitung eines regionalen Polizeipräsidiums, des Polizeipräsidiums Einsatz oder des Landeskriminalamts. Bei Gefahr im Verzug kann eine Maßnahme nach Absatz 1 auch von besonders beauftragten Beamten angeordnet werden. Die Anordnung ergeht schriftlich und ist zu begründen.

(8) Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg ist vor der Einrichtung oder wesentlichen Änderung einer Analyseplattform nach Absatz 1 anzuhören.“

3. Nach § 57 wird folgender § 57a eingefügt:

„§ 57a

Weitere Verarbeitung zu Zwecken der Entwicklung, des Trainings, des Testens, der Validierung und der Beobachtung von informationstechnischen Produkten

(1) Die Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst können bei ihnen vorhandene personenbezogene Daten zur Entwicklung, zum Training, zum Testen, zur Validierung und zur Beobachtung von informationstechnischen Produkten weiter verarbeiten, soweit dies erforderlich ist, insbesondere weil

1. unveränderte Daten benötigt werden oder

2. eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Dabei ist sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Die Nachvollziehbarkeit des verwendeten Verfahrens muss sichergestellt werden, soweit dies technisch möglich ist. Eine weitere Verarbeitung von personenbezogenen Daten, die aus in § 50 genannten Maßnahmen erlangt wurden, ist zu den in Satz 1 genannten Zwecken ausgeschlossen.

(2) Eine Übermittlung von personenbezogenen Daten im Sinne des Absatzes 1 an öffentliche und nichtöffentliche Stellen ist nur zulässig, wenn die empfangende Stelle nachweist, dass die Personen, die die übermittelten Daten weiter verarbeiten sollen, Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder nach dem Verpflichtungsgesetz (BGBl. I 1974, 469, 547) zur Geheimhaltung verpflichtet worden sind.

(3) Die übermittelten Daten sind durch organisatorische und technische Maßnahmen gegen unbefugte Kenntnisnahme zu schützen.“

4. § 74 wird wie folgt geändert:

a) In Absatz 1 wird die Angabe „§§ 48 bis 56“ durch die Angabe „§§ 47a bis 56“ ersetzt.

b) Absatz 2 wird wie folgt geändert:

aa) Folgende Nummer 1 wird eingefügt:

„1. bei Maßnahmen nach § 47a (automatisierte Datenanalyse)

a) die einbezogenen Daten,

b) die verwendeten Suchkriterien sowie

c) die betroffenen Personen, gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden,“.

bb) Die bisherigen Nummern 1 bis 11 werden die Nummern 2 bis 12.

5. § 86 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Die Angabe „§§ 48 bis 56“ wird durch die Angabe „§§ 47a bis 56“ ersetzt.

bb) Folgende Nummer 1 wird eingefügt:

„1. des § 47a (automatisierte Datenanalyse) die betroffenen Personen, gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden,“.

cc) Die bisherigen Nummern 1 bis 11 werden die Nummern 2 bis 12.

b) In Absatz 3 Satz 6 wird die Angabe „§§ 48 bis 56“ durch die Angabe „§§ 47a bis 56“ ersetzt.

6. § 90 wird wie folgt gefasst:

„§ 90

Parlamentarische Kontrolle, Unterrichtung der Öffentlichkeit

(1) Das Innenministerium unterliegt hinsichtlich der nach den §§ 47a, 49, 50, 53, 54 und 55 Absatz 1 erfolgten Maßnahmen sowie den Übermittlungen nach § 61 der Kontrolle durch das Parlamentarische Kontrollgremium. Zu diesem Zweck unterrichtet das Innenministerium das Parlamentarische Kontrollgremium mindestens vierteljährlich. Auf Verlangen des Parlamentarischen Kontrollgremiums hat das Innenministerium zu einer konkreten Maßnahme zu berichten.

(2) Das Innenministerium unterrichtet die Öffentlichkeit in geeigneter Weise jährlich über die Anzahl der in Absatz 1 Satz 1 genannten Maßnahmen.“

7. In § 98 Absatz 1 Nummer 14 wird die Angabe „§§ 48 bis 50“ durch die Angabe „§§ 47a bis 50“ ersetzt.

8. In § 130 Absatz 1 Nummer 1 werden nach den Wörtern „Anordnungsbefugnis gemäß“ die Wörter „§ 47a Absatz 7 Satz 2,“ eingefügt.

9. Die Inhaltsübersicht ist entsprechend anzupassen.

Artikel 2
Änderung der Verordnung des Innenministeriums zur Durchführung des Polizeigesetzes

§ 4 der Verordnung des Innenministeriums zur Durchführung des Polizeigesetzes vom 16. September 1994 (GBl. S. 567), die zuletzt durch Artikel 3 des Gesetzes vom 6. Oktober 2020 (GBl. S. 735, 785) geändert worden ist, wird folgender Absatz 3 angefügt:

„(3) Die Anordnungsbefugnis nach § 47a Absatz 7 Satz 2 PolG kann die Leitung

1. eines regionalen Polizeipräsidiums auf die Leitung des Führungs- und Einsatzstabes, die Leitung der Schutzpolizeidirektion, die Leitung der Kriminalpolizeidirektion und den Polizeiführer vom Dienst,

2. des Landeskriminalamtes auf die Abteilungsleitungen und den Polizeiführer vom Dienst

übertragen.“

Artikel 3
Inkrafttreten

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.

Stuttgart, den

Die Regierung des Landes Baden-Württemberg:

Begründung

A. Allgemeiner Teil

I. Zielsetzung

Das Gesetz verfolgt im Wesentlichen drei Ziele.

Zunächst soll eine Rechtsgrundlage dafür geschaffen werden, bisher unverbundene Daten und Datenquellen des Polizeivollzugsdienstes in einer Analyseplattform zusammenzuführen, um die vorhandenen Datenbestände durch Suchfunktionen systematisch erschließen zu können. Der Polizeivollzugsdienst verfügt über gespeicherte und verarbeitete Daten, die derzeit auf zahlreiche Datenbanken und Quellsysteme verteilt sind. Die daraus entstehenden Datenmengen sind sehr umfangreich, heterogen strukturiert, komplex und zudem oftmals nicht über Schnittstellen miteinander verbunden. Diese Daten bilden regelmäßig die Grundlage für eine Entscheidungsfindung durch den Polizeivollzugsdienst, welche zur Abwehr von Gefahren unerlässlich ist. Eine manuelle Abfrage aus verschiedenen Datenquellen wird durch große Datenmengen und verschiedenste Quellen sowie Dateiformate immer zeitaufwendiger und komplexer. Darüber hinaus müssen die Daten in einem weiteren Schritt aufbereitet und in Beziehung gesetzt werden, bevor eine Analyse erfolgen kann. In zeitkritischen Gefahrenlagen, beispielsweise bei der Verhinderung eines drohenden terroristischen Anschlags, des andauernden sexuellen Missbrauchs zum Nachteil eines Kindes oder einer drohenden schweren Gewalttat, ist die schnelle Reaktionsfähigkeit ein erfolgskritischer Faktor.

Durch Medienbrüche, heterogene Dateiformate und fehlende Beziehungsgeflechte entstehen zeitliche und technische Aufwände, die weder dem aktuellen Entwicklungsstand der Informationstechnik noch den Anforderungen an eine effiziente und effektive Gefahrenabwehr entsprechen. Müssen Daten aus Asservaten in die Entscheidungsfindung durch den Polizeivollzugsdienst miteinbezogen werden, ist die Auswertung ohne Automatisierung in diesen zeitkritischen Situationen nicht zu bewältigen.

Derzeit kann im konkreten Einzelfall nicht ausgeschlossen werden, dass die Polizei Baden-Württemberg im Besitz von relevanten Daten und Informationen ist, diese aber nicht zusammenführen und verwenden kann. Durch eine automatisierte und schnelle Verknüpfung könnten die Daten als Entscheidungsgrundlage mit herangezogen werden.

Für die anlassbezogene automatisierte Datenanalyse soll eine ganzheitliche Plattform zur Verfügung gestellt werden, um polizeiliche Datenbestände effizient und effektiv nach relevanten Informationen auswerten zu können, die auf andere, grundrechtsschonendere Weise nicht gleichermaßen zu gewinnen wären. Sie soll den Abfrageberechtigten als technisches Hilfsmittel zur Verfügung stehen und Daten mit Verknüpfungen durch wenige Suchbefehle visuell aufbereitet darstellen. Die automatisierte Datenanalyse ersetzt nicht die Entscheidungsfindung durch eine menschliche Instanz, sondern erleichtert selbige.

Zudem soll eine Rechtsgrundlage für den Abruf von Standortdaten geschaffen werden, die nach Anwahl der Notrufnummer mittels eines mobilen Endgerätes automatisiert und ohne Interaktion der anrufenden Person anfallen. Dies ermöglicht dem Polizeivollzugsdienst unter Nutzung der sogenannten AML-Technologie die schnelle Standortbestimmung einer hilfesuchenden Person. Aufgrund der mit einem Notfall einhergehenden Stresssituation wissen hilfesuchende Personen oftmals nicht genau, wo sie sich befinden, können bei Sprachbarrieren ihren Standort nicht mitteilen oder haben aus medizinischen oder sonstigen Gründen eine eingeschränkte räumliche Orientierung. Auch eine plötzlich unterbrochene Notrufverbindung kann dafür sorgen, dass notrufende Personen ihren Standort nicht mitteilen können. Diese Umstände kosten wertvolle Zeit und können die rechtzeitige Ankunft von Polizeivollzugsdienst oder Rettungskräften gefährden. Zur Verbesserung der Standortbestimmung von Mobilfunkteilnehmenden im Rahmen der polizeilichen Notrufbearbeitung ist daher eine genaue, schnelle und technisch zeitgemäße Übermittlung des Standorts hilfesuchender Personen erforderlich.

Schließlich soll eine Rechtsgrundlage zur Verarbeitung von Daten bei der Entwicklung, dem Training, dem Testen, der Validierung und der Beobachtung von informationstechnischen Produkten außerhalb von rein wissenschaftlichen Forschungsarbeiten geschaffen werden. Erfolgreiche Polizeiarbeit erfordert moderne und sachgerechte polizeiliche Befugnisse und vor dem Hintergrund der zunehmenden Digitalisierung auch den Einsatz neuer Technologien – unter anderem solcher, die mit Künstlicher Intelligenz (KI) im Sinne der 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 (KI-VO) ausgestattet sind. Gerade KI-Anwendungen benötigen jedoch zur Entwicklung und zum Testen realitätsnahe Trainingsdaten. Eine zielgerichtete Entwicklung und Validierung ist daher in vielen

Fällen nur durch die Nutzung polizeispezifischer – in aller Regel auch personenbezogener – Daten möglich.

Damit informationstechnische Systeme einschließlich KI-Systemen und KI-Modellen im Sinne der KI-VO ordnungsgemäß getestet und trainiert werden können, bedarf es zur Verarbeitung personenbezogener Daten einer entsprechenden Rechtsgrundlage. § 57 PolG beschränkt sich auf die Datenverarbeitung bei der Durchführung wissenschaftlicher Forschungsarbeiten, wobei der eng auszulegende Forschungsbegriff im Sinne der Datenschutz-Grundverordnung (DSGVO) und der Datenschutzkonferenz (DSK) primär wissenschaftlich ausgerichtete, methodisch fundierte und vom operativen Zweck losgelöste Vorhaben erfasst. Es ist daher durchaus fraglich, inwieweit praxisnahe Entwicklungen, systematische Tests oder die erprobungsweise Nutzung polizeilicher Software, die auf einen späteren Echtbetrieb abzielen, von der bestehenden Regelung erfasst werden.

Durch die Rechtsgrundlage zur Verarbeitung von Daten bei der Entwicklung, dem Training, dem Testen, der Validierung und der Beobachtung von informationstechnischen Produkten einschließlich KI-Systemen und KI-Modellen im Sinne der KI-VO außerhalb von rein wissenschaftlichen Forschungsarbeiten werden die Voraussetzungen für eine eigenständige Entwicklung von informationstechnischen Produkten durch die Polizei Baden-Württemberg geschaffen. Sie dient daher insbesondere auch dazu, durch unabhängige Konzeption und Entwicklung von informationstechnischen Produkten die Abhängigkeit von ausländischen bzw. außereuropäischen Produkten zu reduzieren.

II. Wesentlicher Inhalt

Mit der neu aufgenommenen Regelung in § 47a PolG wird eine bereichsspezifische Ermächtigung für die Anwendung einer automatisierten Datenanalyse geschaffen. Die informationstechnische Entwicklung der letzten Jahre ermöglicht es, bisher unverbundene Daten und Datenquellen auf einer Analyseplattform zusammenzuführen und die vorhandenen Datenbestände durch Suchfunktionen systematisch zu erschließen.

In seinem Urteil vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20) hat das Bundesverfassungsgericht grundsätzlich geklärt, unter welchen Voraussetzungen eine automatisierte Datenanalyse verfassungskonform geregelt werden kann.

Die Verarbeitung gespeicherter personenbezogener Daten im Rahmen einer automatisierten Datenanalyse greift in das Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG in zweifacher Weise ein. Zum einen stellt die Nutzung der Daten über den ursprünglichen Anlass hinaus einen neuen Grundrechtseingriff dar, der nach dem Grundsatz der Zweckbindung gerechtfertigt sein muss. Zum anderen hat das Bundesverfassungsgericht ein potentielles Eigengewicht der automatisierten Datenanalyse festgestellt, das über das Eingriffsgewicht der weiteren Verwendung vormals getrennter Daten hinausgeht (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 50, 67 ff.). Für eine verfassungskonforme Ausgestaltung der automatisierten Datenanalyse ist eine Bestimmung dieses Eigengewichts erforderlich, das je nach Art und Umfang der einzubeziehenden Daten und der Methode der Analyse sehr unterschiedlich sein kann (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 72 ff.). Die gesetzlichen Anforderungen für eine verfassungskonforme Regelung bestimmen sich daher nach dem Eingriffsgewicht, das vom Gesetzgeber durch Vorkehrungen und Schutzmaßnahmen beeinflusst werden kann.

Die neu aufgenommene Regelung in § 45a PolG ermöglicht dem Polizeivollzugsdienst unter Nutzung der AML-Technologie die schnelle und sichere Standortbestimmung einer hilfesuchenden Person. Aufgrund europarechtlicher Vorgaben werden die Standortdaten mobiler Endgeräte bei Anwahl einer nationalen Notrufnummer automatisiert erhoben. Hierfür kommt der auf mobilen Endgeräten vorinstallierte Systemdienst AML zum Einsatz. Zuständig für die Annahme von Notrufen sind in Deutschland die sogenannten Notrufabfragestellen (vgl. § 164 Telekommunikationsgesetz, § 2 Nummer 2 Notrufverordnung). Für die Notrufnummer 110 sind die Polizeien der Länder zuständige Notrufabfragestelle.

Mit der neu aufgenommenen Regelung in § 57a wird eine Grundlage für die Verarbeitung von personenbezogenen Daten für die Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von informationstechnischen Produkten einschließlich KI-Systemen und KI-Modellen im Sinne der KI-VO geschaffen, unabhängig von der Durchführung wissenschaftlicher Forschungsarbeiten.

III. Alternativen

Alternativen zu einer gesetzlichen Regelung bestehen nicht.

IV. Finanzielle Auswirkungen

Mit der Umsetzung der durch die Änderung des Polizeigesetzes geschaffenen Rechtsgrundlagen für die automatisierte Datenanalyse und zur Verarbeitung von Standortdaten bei Anwahl der Notrufnummer sind Mehrausgaben für den Landeshaushalt in Höhe von jährlich insgesamt rd. 10 Mio. EUR verbunden. Für die automatisierte Datenanalyse ist ein Bedarf in Höhe von 9,25 Mio. EUR für Personal- und Sachmittel veranschlagt. Neben den Kosten zur Beschaffung der Spezialsoftware sind für den Betrieb der technisch komplexen informationstechnischen Infrastruktur informationstechnische Spezialisten einzustellen. Für den Betrieb der AML-Technologie werden Finanzmittel in Höhe von rd. 550.000 EUR benötigt. Im Staatshausplan 2025/2026 wurde diese Mittelbedarfe bereits entsprechend berücksichtigt und im Bereich des Innenministeriums etatisiert. Hinsichtlich der Schaffung einer Rechtsgrundlage für die Verarbeitung von Daten bei der Entwicklung, dem Training, dem Testen, der Validierung und der Beobachtung von informationstechnischen Produkten einschließlich KI-Systemen und KI-Modellen im Sinne der KI-VO außerhalb von rein wissenschaftlichen Forschungsarbeiten entstehen für Softwarebeschaffung, -entwicklung und -erprobung sächliche und personelle Aufwände, die in den Folgejahren von Anzahl und Ausgestaltung der Anwendungen abhängig sein werden und sich daher noch nicht beziffern lassen. Der Polizei stehen Mittel im Rahmen der informationstechnischen Budgetplanung im Staatshaushaltsplan zur Verfügung. Diese Mittel können in Teilen für die Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von informationstechnischen Produkten einschließlich KI-Systemen und KI-Modellen im Sinne der KI-VO genutzt werden.

V. Bürokratievermeidung, Prüfung der Vollzugstauglichkeit

Auf eine Bürokratielastenschätzung und einen Praxis-Check wurde gemäß Nummern 4.3.3 und 4.3.4 der Verwaltungsvorschrift der Landesregierung und der Ministerien zur Erarbeitung von Regelungen (VwV Regelungen) verzichtet, da durch das vorliegende Gesetz weder erhebliche Auswirkungen für Unternehmen, Verwaltung und Bürgerinnen und Bürger noch aufwendige Verwaltungsverfahren zu erwarten sind. Gleichwohl können punktuell Mehraufwände beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen seiner gesetzlichen Zuständigkeit durch Beratungsleistungen und aufsichtliche Kontrolle zum Zwecke der Überprüfung der Einhaltung gesetzlicher Vorgaben entstehen, die im Rahmen vorhandener Mittel gedeckt werden.

VI. Nachhaltigkeitscheck

Der Nachhaltigkeitscheck lässt keine nennenswerten Auswirkungen des Gesetzesvorhabens auf die ökonomischen, ökologischen und sozialen Verhältnisse erwarten. Lediglich der Zielbereich IV.2. Bedürfnisse und gutes Leben – Wohl und Zufriedenheit – der Anlage 2 zur VwV Regelungen ist tangiert. Der Gesetzentwurf leistet einen Beitrag, um die Sicherheit in der Bevölkerung zu verbessern. Er ist mit den Zielen einer nachhaltigen Entwicklung vereinbar.

VII. Digitaltauglichkeitscheck

Die automatisierte Datenanalyse ermöglicht es dem Polizeivollzugsdienst, vorhandene Datenbestände durch Suchfunktionen systematisch zu erschließen. Dadurch werden Medienbrüche reduziert und manuelle Abfragen verschiedener Datenquellen entbehrlich, die aufgrund großer Datenmengen aus unterschiedlichen Quellen sowie unterschiedlicher Dateiformate bislang zeitaufwendig und komplex sind. Die automatisierte Datenanalyse erfolgt mittels eines elektronischen Fachverfahrens. Zur Verringerung der Eingriffsintensität der automatisierten Datenanalyse steht ihre Nutzung bzw. damit korrespondierend die Verlängerung entsprechender Speicherfristen unter Anordnungsvorbehalt. Diese Anordnungen erfolgen schriftlich außerhalb des elektronischen Fachverfahrens. Die vorgegebene Schriftform und der damit einhergehende Medienbruch tragen als bewusste Zäsur dem hohen Eingriffsgewicht einer automatisierten Datenanalyse in das Recht auf informationelle Selbstbestimmung Rechnung. Sie dienen der rechtlichen Absicherung und gewährleisten eine effektive aufsichtliche Kontrolle.

Durch Nutzung der AML-Technologie wird das Verfahren zur schnellen Standortbestimmung einer hilfesuchenden Person mittels einer Web-Anwendung digitalisiert und Medienbrüche reduziert. Zudem wird die Genauigkeit der Standortbestimmung durch die kombinierte Nutzung verschiedener technischer Positionsdienste erheblich verbessert. Die Übermittlung der Standortdaten vom AML-Endpunkt zur Notrufabfragestelle erfolgt auf deren Abruf vollautomatisiert.

Durch die Einführung entsprechender elektronischer Fachverfahren ist daher sowohl bezogen auf die Analyse von polizeilichen Datenbeständen als auch bezogen auf die Standortbestimmung von notrufenden Personen eine Beschleunigung der polizeilichen Abläufe zu erwarten.

VIII. Sonstige Kosten

Nennenswerte Kosten für Private entstehen durch die Gesetzesänderungen nicht.

B. Einzelbegründung

Zu Artikel 1 - Änderung des Polizeigesetzes:

Zu Nummer 1:

§ 45a Absatz 1 regelt die Einrichtung eines „AML-Endpunktes“ beim Präsidium Technik, Logistik, Service der Polizei. Bei AML handelt sich um einen Systemdienst, der fest in das Betriebssystem (i. d. R. Android oder iOS) der mobilen Endgeräte integriert ist. Dabei wird neben dem Rufaufbau zur Notrufabfragestelle zusätzlich (ohne Zutun der anrufenden Person) die Satellitennavigation, die GPS-Standortübertragung sowie das WLAN (zur Verbesserung der Standortgenauigkeit) des mobilen Endgerätes selbstständig aktiviert und gemäß technischem Bericht ETSI TR 103 393 V1.1.1 (2016-03) des Europäischen Instituts für Telekommunikationsnormen (ETSI) der Gerätestandort, Datum und Uhrzeit der Standortbestimmung, die Mobilfunkzellenidentifikationsnummer (Cell-ID), die internationale mobile Teilnehmerkennung (IMSI), die internationale Mobilgerätekennung (IMEI), der Mobilländercode (MCC), der Mobilnetzcode (MNC) sowie die Mobilfunknummer übermittelt. Nach Satz 1 hält das Präsidium Technik, Logistik, Service der Polizei die von Betriebssystemherstellern übermittelten Daten zum Zwecke des dezentralen Abrufs durch die zuständigen Notrufabfragestellen der Polizeien der Länder vor. Im Verhältnis zu den Polizeien der anderen Länder wird das Präsidium Technik, Logistik, Service der Polizei als Auftragsverarbeiter tätig. Hierzu sind separate Auftragsverarbeitungsvereinbarungen mit den einzelnen Ländern zu schließen. Die Speicherdauer wird durch Satz 2 auf 60 Minuten begrenzt. AML dient ausschließlich der Rettung von Personen in Notlagen und wird nur bei Anwahl der Notrufnummer aktiviert. Satz 3 stellt sicher, dass eine Verarbeitung der Daten zu einem anderen Zweck als zur Übermittlung an die Notrufabfragestellen unzulässig ist.

Absatz 2 regelt die Erhebung, Verarbeitung und Speicherung von AML-Daten durch die zuständigen Notrufabfragestellen. In Baden-Württemberg ist dies der Polizeivollzugsdienst. Die Verarbeitung ist ausschließlich zum Zweck der Abwehr einer Gefahr für Leib, Leben oder Freiheit möglich. Satz 2 begrenzt die Speicherdauer der Daten auf sechs Monate. Die Speicherung der AML-Daten erfolgt technisch im Einsatzleitsystem (derzeit Viadux). Die Löschfrist orientiert sich daher an dessen Löschkonzept.

Zu Nummer 2:

§ 47a Absatz 1 regelt die Eingriffsschwellen und definiert eine automatisierte Datenanalyse. Dabei besteht das technische Verfahren aus zwei aufeinander aufbauenden, aber praktisch zeitgleich stattfindenden Schritten, nämlich dem Zusammenführen unterschiedlicher Dateisysteme und der sich daran anschließenden Recherche innerhalb der zusammengeführten Datenbestände. Der erste Schritt überwindet das strukturelle Problem, dass in den Beständen der Polizei Baden-Württemberg Daten in unterschiedlichen Formaten und getrennten Dateien gespeichert und damit nicht im selben Bearbeitungskontext einheitlich verfügbar sind. Der zweite Schritt beschreibt die eigentliche Analyse, die in einer Verknüpfung, Abgleichung, Aufbereitung, Auswertung und Bewertung der zusammengeführten Datenbestände besteht.

Eine automatisierte Datenanalyse, also die Zusammenführung, Verknüpfung, Abgleichung, Aufbereitung, Auswertung und Bewertung von Datenbeständen auf einer Analyseplattform, stellt eine komplexere Form des Datenabgleichs als die einfache Suche nach Übereinstimmungen zwischen einzelnen, bisher unverbundenen Datensätzen dar (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 91 ff.).

Absatz 1 beschreibt in den Nummern 1 bis 3 unterschiedliche Eingriffsschwellen, die Anlass für eine automatisierte Datenanalyse sein können. Die Eingriffsschwellen sind zum jeweiligen Eingriffsgewicht der automatisierten Datenanalyse in Beziehung zu setzen, damit die Verhältnismäßigkeit der Maßnahme gewahrt bleibt. Beim Einsatz einer automatisierten Datenanalyse ist der Verhältnismäßigkeitsgrundsatz im besonderen Maße zu berücksichtigen. Es muss sichergestellt werden, dass kein milderes Mittel zur Verfügung steht, welches zur Wahrnehmung der polizeilichen Aufgabe ebenso geeignet wäre und den Einzelnen oder die Allgemeinheit voraussichtlich weniger beeinträchtigen würde.

Die Eingriffsschwelle in Absatz 1 Nummer 1 ist an enge Voraussetzungen geknüpft, wie sie allgemein für eingriffsintensive Maßnahmen gelten. Vorausgesetzt wird eine konkrete Gefahr für ein besonders gewichtiges Rechtsgut. Der Begriff der konkreten Gefahr setzt eine Sachlage voraus, die bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens im Einzelfall in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einer Verletzung des geschützten Rechtsguts führt. Da der Eingriffsanlass mit dem Erfordernis einer konkreten Gefahr streng begrenzt ist und nur besonders gewichtige Rechtsgüter geschützt werden, darf das Eingriffsgewicht der automatisierten Datenanalyse unter diesen Voraussetzungen vergleichsweise hoch sein.

Die Eingriffsschwelle in Absatz 1 Nummer 2 erlaubt weniger gewichtige Eingriffe, die nach der Rechtsprechung des Bundesverfassungsgerichts beim Vorliegen einer konkretisierten Gefahr bereits dann zu rechtfertigen sind, wenn sie dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht dienen, wie dies bei der Verhütung von Straftaten von zumindest erheblicher Bedeutung der Fall ist (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 107). Das Eingriffsgewicht wird zusätzlich durch die Voraussetzung verringert, dass die zugrundeliegende Anlasstat nicht nur abstrakt, sondern auch im Einzelfall schwer wiegen muss. Eine hinreichend konkretisierte Gefahr kann schon vorliegen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen darauf hinweisen, dass eine entsprechende Straftat begangen werden wird. Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 106). Da zu den Straftaten von erheblicher Bedeutung auch Vorfeldstraftaten wie die §§ 129a und 129b Strafgesetzbuch (StGB) sowie die §§ 89a, 89b und 89c StGB gehören, wird in der Nummer 2 zusätzlich verlangt, dass mit der konkretisierten Gefahr der Begehung einer Straftat von erheblicher Bedeutung auch bereits eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut verbunden ist (vgl. BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 170; BVerfG, Beschluss vom 9. Dezember 2022, 1 BvR 1345/21, Rn. 95).

Die Eingriffsschwelle in der Nummer 3 betrifft die Verhütung von Straftaten. Dies ist bei weniger gewichtigen Eingriffen zulässig, wenn sie dem Schutz besonders gewichtiger Rechtsgüter dienen (BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 107). Dabei muss der Gesetzgeber das erforderliche Rechtsgut nicht zwingend unmittelbar benennen, sondern kann auch an entsprechende Straftaten anknüpfen. In Anlehnung an die vom Bundesverfassungsgericht in seinem Urteil zur akustischen Wohnraumüberwachung entwickelte (BVerfG, Urteil vom 3. März 2004 – 1 BvR 2378/98 – Rn. 238) und bis heute fortgeschriebene (vgl. BVerfG, Beschluss vom 09.12.2022 – 1 BvR 1345/21 – Rn. 179) und damit verfestigte Nomenklatur sind besonders schwere Straftaten solche, die mit einer Höchststrafe von mindestens zehn Jahren Freiheitsstrafe bedroht sind. Maßgeblicher Anknüpfungspunkt für die Einordnung ist der abstrakte Strafrahmen, wie er vom Gesetzgeber für eine bestimmte Straftat festgelegt wird

(BVerfG, Urteil vom 3. März 2004, a.a.O., Rn. 237 f.). Praktisch relevant ist in weiten Teilen der Straftatenkatalog des § 100b Absatz 2 der Strafprozessordnung (StPO).

Absatz 2 regelt die zulässige Methode einer automatisierten Datenanalyse und stellt klar, dass es sich hierbei um ein technisches Hilfsmittel handelt, das die bisherige Arbeitsweise des Polizeivollzugsdienstes erleichtert, ohne sie grundlegend zu verändern. Die Analyseplattform darf keine Prognosesoftware in dem Sinne sein, dass sie eigenständig kriminelles Verhalten vorhersagt und die von einem Menschen zu treffende abschließende Bewertung ersetzt. Sie darf lediglich ein technisches Hilfsmittel sein, das den Polizeivollzugsdienst bei seiner Aufgabenwahrnehmung unterstützt, indem Informationen aus verschiedenen Dateisystemen zusammengeführt werden. Die abschließende Bewertung der zusammengeführten Informationen ist und bleibt Aufgabe des Polizeivollzugsdienstes. Absatz 2 Satz 1 legt fest, dass die automatisierte Datenanalyse den Polizeivollzugsdienst bei der Erfüllung seiner Aufgaben unterstützt, indem sie Informationen bereitstellt, die es dem Polizeivollzugsdienst ermöglichen, eigene Bewertungen, Prognosen und Entscheidungen zu treffen. Der Mensch – und nicht der Algorithmus – bewertet die bereitgestellten Informationen abschließend. Damit sind beispielsweise alleinige maschinelle Gefährlichkeitsbewertungen zu Personen unzulässig. Die abschließende Bewertung, ob eine bestimmte Person mit hoher Wahrscheinlichkeit künftig Straftaten begehen wird, trifft ein Mensch und nicht der Algorithmus.

Aufgrund der voranschreitenden technologischen Entwicklung ist es für eine effiziente Gefahrenabwehr erforderlich, den Rechtsrahmen auszuschöpfen, der insbesondere durch die KI-VO vorgegeben wird. Gemeint ist die Anwendung von KI-Systemen und KI-Modellen im Sinne und insbesondere unter Berücksichtigung der Einschränkungen und Vorgaben der KI-VO.

Die KI-Systeme und KI-Modelle können die automatisierte Anwendung zur Datenanalyse ergänzen, um beispielsweise

- diverse Datenformate schneller zusammenzuführen,

- Tat- und Täternetzwerke schneller zu identifizieren,

- Hinweise aus unstrukturierten Daten schneller zu erkennen und mit den vorhandenen polizeilichen Informationen abzugleichen oder

- komplexe Analyseschritte zu vereinfachen und für die Polizeibehörden nutzbar zu machen.

Welche Systeme mit oder ohne KI-Funktionalität letztlich in eine verfahrensübergreifende Recherche- und Analyseplattform integriert werden, kann aufgrund der fortschreitenden technischen Entwicklungen im Einzelnen nicht konkret abgesehen werden.

Vor dem Hintergrund des hohen Eingriffsgewichts einer automatisierten Datenanalyse sind die inhärenten Risiken der KI-unterstützten Durchführung solcher Maßnahmen sowie der angebundenen KI-Systeme oder KI-Modelle besonders zu berücksichtigen.

Mit Satz 2 wird hervorgehoben, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden dürfen.

Satz 3 schreibt ausdrücklich fest, dass abschließende maschinelle Sachverhaltsbewertungen verboten sind, und steht dabei in Bezug zu der allgemeingültigen Regelung des Verbots von automatisierten Entscheidungsfindungen in § 84 PolG. Die abschließende Bewertung der bereitgestellten Informationen und eine Entscheidung über hierauf aufbauende weitere Maßnahmen bleiben dem Polizeivollzugsdienst vorbehalten.

Satz 4 sichert die Funktion der Analyseplattform als bloßes Hilfsmittel für die polizeiliche Aufgabenwahrnehmung ab, indem klargestellt wird, dass die automatisierte Datenanalyse manuell ausgelöst wird. Aus dem Zusammenspiel der Sätze 3 und 4 ergibt sich, dass der Mensch am Anfang und am Ende des Entscheidungsprozesses steht. Mit Satz 4 wird außerdem die Methode des Suchvorgangs näher konkretisiert. Auch dies dient der Minderung des Eingriffsgewichts. Wie sich aus der Entscheidung des Bundesverfassungsgerichts ergibt, ist das Eingriffsgewicht umso höher, je offener die Methode des Suchvorgangs gestaltet ist (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 93). Die mit einer offenen Suche verbundenen Gefahren können durch eine Einschränkung der Datenverarbeitungsmethode gesenkt werden, wenn der Suchvorgang eingrenzend so geregelt ist, dass er einen Bezug zu einem konkreten Suchanlass voraussetzt (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 95). Dementsprechend wird in Satz 4 geregelt, dass die automatisierte Datenanalyse anhand anlassbezogener und zielgerichteter Suchkriterien erfolgt. In den Fällen des Absatzes 1 Nummern 2 und 3 ist der Suchvorgang zudem auf die in den §§ 6 und 7

PolG genannten Personen auszurichten. Hierdurch wird das Eingriffsgewicht weiter gemindert, weil mit dem Erfordernis einer tatsachengestützten Verbindung zu einer konkret verantwortlichen Person das Risiko sinkt, dass Personen in weitere polizeiliche Maßnahmen einbezogen werden, die dafür keinen zurechenbaren Anlass gegeben haben (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 94). Die Beschränkung dieser zusätzlichen begrenzenden Vorgabe auf die Fälle des Absatzes 1 Nummern 2 und 3 ist dem Umstand geschuldet, dass die Eingriffsschwelle hier im Vergleich zu Absatz 1 Nummer 1, bei dem eine konkrete Gefahr für besonders gewichtige Rechtsgüter verlangt wird, niedriger liegt. Während nach Absatz 1 Nummer 2 als Eingriffsanlass eine konkretisierte Gefahr für weniger gewichtige Rechtsgüter ausreicht, erlaubt Absatz 1 Nummer 3 die automatisierte Datenanalyse bereits im Vorfeld einer konkretisierten Gefahr. Zur Wahrung der Verhältnismäßigkeit muss die Eingriffsintensität der Maßnahme daher reduziert werden, was hier durch eine weitere Konkretisierung der Suchkriterien erfolgt.

Mit dem Ausrichten der Maßnahme auf die in den §§ 6 und 7 PolG genannten Personen in Satz 5 ist gemeint, dass sich der Suchvorgang nur auf die genannten Personengruppen beziehen darf. Die Einschränkung ist – auf Grundlage der Entscheidung des Bundesverfassungsgerichts vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20) – so zu verstehen, dass eine tatsachengestützte Verbindung zu einer konkret verantwortlichen Person gegeben sein muss. Ein solcher Bezug darf nicht erst durch die Maßnahme hergestellt werden, da ansonsten das Risiko steigt, dass Personen in weitere polizeiliche Maßnahmen einbezogen werden, die dafür keinen zurechenbaren Anlass gegeben haben. Der Begriff des „Ausrichtens“ stellt dabei im Gesamtkontext darauf ab, dass lediglich Personen, die für die Begehung von Straftaten von auch im Einzelfall erheblicher Bedeutung (§ 47a Absatz 1 Nummer 2 i.V.m. § 49 Absatz 3 PolG) oder für die Begehung von besonders schweren Straftaten verantwortlich sind, Anlass für eine Suche geben können. Sofern es sich hierbei um eine Gruppe handelt, kann auch dies Anlass für die Suche sein.

Satz 6 enthält ein ausdrückliches Verbot der direkten Anbindung der Analyseplattform an Internetdienste. Dies dient der Eingriffsminimierung, weil eine Verknüpfung der Analyse- oder Auswerteeinrichtung die Verarbeitung besonders großer Datenmengen praktisch fördert (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 88). Grundsätzlich dürfen nur die von der Polizei Baden-Württemberg gespeicherten Daten in die Analyseplattform einbezogen werden, was zu einer Begrenzung der auswertbaren Datenmenge beiträgt. Nur im Einzelfall können – soweit erforderlich – die bei der Bearbeitung eines konkreten Fallkomplexes gezielt

ermittelten und gespeicherten Daten, die bei einer Internetrecherche angefallen sind, in die automatisierte Datenanalyse gemäß Absatz 3 Satz 2 einbezogen werden.

Absatz 3 bestimmt abschließend, welche Datenbestände und Daten auf der Analyseplattform zusammengeführt werden dürfen. Das Gesetz begrenzt damit sowohl den Umfang als auch die Art der verarbeitbaren Daten, wodurch das Eingriffsgewicht der automatisierten Datenanalyse gemindert wird (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 78). Dabei wird zwischen Datenbeständen unterschieden, die auf der Plattform laufend zusammengeführt werden, und solchen Daten, die einzelfallbezogen in die Analyse einbezogen werden.

Nach Satz 1 können zum Zweck der automatisierten Datenanalyse eigene Vorgangsdaten, Falldaten, Daten aus polizeilichen Auskunftssystemen und Daten aus dem polizeilichen Informationsaustausch zusammengeführt werden. Die positive Benennung der zum Zweck der automatisierten Datenanalyse nutzbaren Quellen hat den Charakter einer abschließenden Regelung und enthält damit gleichzeitig eine Begrenzung der Datenmenge (vgl. BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 78). Die zusätzliche Einschränkung auf eigene Daten stellt klar, dass es sich um Daten handelt, welche die Polizei Baden-Württemberg als verantwortliche Stelle in den eigenen polizeilichen Dateisystemen gespeichert hat.

Vorgangsdaten sind sämtliche Unterlagen, die im Zusammenhang mit einer polizeilichen Tätigkeit bei einem bestimmten Einsatzanlass zu Personen und Sachen im polizeilichen Vorgangsbearbeitungssystem erfasst werden. Aufgenommen werden insbesondere Anzeigen, Ermittlungsberichte und Vermerke, die nicht nur Daten zu Verdächtigen, Beschuldigten oder sonstigen Anlasspersonen enthalten, sondern beispielsweise auch zu Personen, die Anzeige erstatten, Hinweise geben oder Zeuginnen oder Zeugen sind. Die Vorgangsdaten umfassen Vorgangssachbearbeitungsdaten und Vorgangsverwaltungsdaten gleichermaßen, wobei Vorgangsverwaltungsdaten in der Regel bereits keine Relevanz für entsprechende Analysen haben dürften. Da die Daten aus der Vorgangsverwaltung typischerweise auch viele Unbeteiligte betreffen, wird in Absatz 6 Satz 3 geregelt, dass deren Vorgangsdaten nicht in die automatisierte Datenanalyse einbezogen werden dürfen. Hierdurch wird die Eingriffsintensität reduziert.

Falldaten in Fallbearbeitungssystemen dienen der Unterstützung von Ermittlungs- und Recherchetätigkeiten sowie Auswertungen bei komplexen, fallübergreifenden Ermittlungen oder bei Strukturermittlungen. Ein Fallbearbeitungssystem geht über die reine Verwaltung von Vorgangsdaten hinaus, indem es der Anwenderin oder dem

Anwender ein speziell auf die Aufhellung von Strukturen hin ausgerichtetes Werkzeug zur Verfügung stellt und vor allem Beziehungen zwischen Personen, Institutionen, Objekten und Sachen abbildet. Fallbearbeitungssysteme können sowohl zu präventiven als auch zu repressiven Zwecken eingesetzt werden. Sie enthalten überwiegend Daten von Anlasspersonen und deren Kontaktpersonen aus strafrechtlichen Ermittlungsverfahren. Anlasspersonen sind verurteilte, beschuldigte oder verdächtige Personen oder Personen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie in naher Zukunft Straftaten von erheblicher Bedeutung begehen.

Polizeiliche Auskunftssysteme enthalten personenbezogene Informationen, die sowohl zum Zweck der Verhütung von Straftaten als auch zum Zweck der Strafverfolgung und -vollstreckung gespeichert werden. Das polizeiliche Auskunftssystem der baden-württembergischen Polizei besteht aus unterschiedlichen Datengruppen. Hierzu gehören insbesondere:

- Kriminalaktennachweise: Diese beinhalten Informationen über laufende und abgeschlossene Ermittlungsverfahren, insbesondere die Straftatbestände, wegen derer ermittelt wurde, Datum und Art der Einstellungsverfügung, deren Gründe, Angaben zur Anklageerhebung sowie zum Ausgang des Hauptverfahrens.

- Personenfahndung: Diese listet in einem Katalog den Anlass und den Zweck der Ausschreibung einer Person zur Fahndung mit dem Ziel auf, fahndungsrelevante Erkenntnisse über Täterinnen oder Täter, Tathergang, Zeuginnen oder Zeugen, Geschädigte etc. zu erlangen. Die Personenfahndung dient unter anderem der Festnahme oder Aufenthaltsermittlung von Straftäterinnen oder Straftätern (Strafverfolgung) oder dem Schutz von vermissten Personen (Gefahrenabwehr) sowie der Strafvollstreckung von verurteilten Personen bzw. der Verhinderung einer Wiedereinreise von verurteilten Personen, die nach Teilverbüßung ihrer Haftstrafe ins Ausland abgeschoben oder überstellt wurden.

- Sachfahndung: Sie dient unter anderem der Beweissicherung sowie der Ermittlung der Eigentümer bzw. Besitzer von Sachen, die durch eine Straftat oder auf andere Weise abhandengekommen sind.

- Haftdatei: Sie beinhaltet Daten von Personen, die wegen einer rechtswidrigen Tat einer richterlich angeordneten Freiheitsentziehung unterliegen.

- Erkennungsdienst und DNA-Analyse-Datei: Die Erfassung und Speicherung von biometrischen Merkmalen (insbesondere Fingerabdrücke, Lichtbilder und DNA - Identifizierungsmuster) bilden die Grundlage für die Ermittlung von Täterinnen oder Tätern in Strafverfahren, die Zuordnung von Tatortspuren, das Erkennen von Tat-/Täter-Zusammenhängen, aber auch die Identifizierung von hilflosen Personen oder unbekannten Toten. Die aus der DNA-Analyse nach § 81g StPO gewonnenen Identifizierungsmuster werden in einer zentralen DNA-Analyse-Datei (DAD) bundesweit gespeichert.

Polizeiliche Auskunftssysteme unterstützen den zügigen Informationsaustausch und die Erkenntnisgewinnung über bereits einschlägig in Erscheinung getretene Straftäterinnen oder Straftäter und dienen als Grundlage der Personenüberprüfung und Identifizierung im Rahmen der Aufklärung fahndungsrelevanter Sachverhalte, etwa bei offenen Fahndungsausschreibungen aufgrund von Haftbefehlen oder auch bei Vermisstenfahndungen. Darüber hinaus dienen die Daten der Eigensicherung bei polizeilichen Einsatzanlässen. Durch die Einbeziehung dieser Daten in die automatisierte Datenanalyse können beispielsweise Mittäterinnen oder Mittäter identifiziert, Tatbeteiligungen anhand der Haftdaten auch ausgeschlossen, bestehende Verbindungen visualisiert sowie ein Abgleich mit anderen Datenquellen durchgeführt werden.

Daten aus dem polizeilichen Informationsaustausch sind zwischen den Polizeien des Bundes und der Länder ausgetauschte polizeiliche Informationen mit hoher Relevanz insbesondere zu überregionalen Straftätern, zu serienmäßig begangenen Straftaten oder zu akuten Gefahrensachverhalten. Derzeit wird hierfür überwiegend das bundesweite webbasierte Fernschreibsystem EPOST 810 genutzt.

Absatz 3 Satz 2 regelt neben der ergänzenden Einbeziehung von Verkehrsdaten und Daten aus Asservaten auch die Einbeziehung von Daten aus gezielten Abfragen bei anderen Polizeien, von Daten aus gesondert geführten staatlichen Registern und von einzelnen gesondert gespeicherten Datensätzen aus Internetquellen.

Mit dem Begriff der Verkehrsdaten werden gemäß der Legaldefinition in § 3 Nummer 70 TKG diejenigen Daten erfasst, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind. Hierzu gehören insbesondere auch die für die Polizeiarbeit praktisch bedeutsamen Verbindungsdaten einschließlich Standortdaten (vgl. § 9 Absatz 1 Nummer 1 TDDDG), die durch Telekommunikationsüberwachungsmaßnahmen gem. § 100a StPO, durch Funkzellenabfragen gemäß § 100g Absatz 3 StPO bzw. für

kennungsbezogene Verkehrsdatenabfragen gemäß § 100g Absatz 1 und 2 StPO oder unter Einsatz eines IMSI-Catchers auf der Grundlage des § 100i Absatz 1 Nummer 2 StPO erhoben werden können. Im präventiven Bereich können Verkehrsdaten einschließlich Standortdaten kennungsbezogen oder über eine Funkzellenabfrage nach § 53 PolG, durch Auskünfte des Telekommunikationsanbieters nach §§ 52, 54 PolG oder durch den Einsatz eines IMSI-Catchers nach § 55 Absatz 1 PolG erlangt werden. Die Kenntnis darüber, welches mobile Telekommunikationsendgerät zu einem bestimmten Zeitpunkt an einem bestimmten Ort angemeldet war, kann für die polizeiliche Gefahrenabwehr von wesentlicher Bedeutung sein, weil der Aufenthaltsort des Nutzers eines Telekommunikationsendgerätes zum Beispiel Aufschlüsse über Organisationsstrukturen einer Gruppierung geben kann oder die Beteiligung einer Person ausschließen und sie damit entlasten kann.

Daten aus Asservaten sind aus sichergestellten oder beschlagnahmten Datenträgern extrahierte Daten oder Scans papierhafter Asservate. Datenträger dieser Art können beispielsweise USB-Sticks, Festplatten, Smartphones oder Laptops sein. Das Einbeziehen von Asservaten ist im Einzelfall dann möglich, wenn mindestens tatsächliche Anhaltspunkte dafür vorliegen, dass das einzubindende Asservat in Verbindung zum konkreten Suchanlass steht.

Daten anderer Polizeien sind nicht von Satz 1 umfasst. In gezielten Einzelabfragen erhobene Daten, die andere Polizeien als verantwortliche Stelle in ihren polizeilichen Dateisystemen gespeichert haben, können über Satz 2, soweit erforderlich, ergänzend in die Analyse einbezogen werden.

Daten aus staatlichen Registern sind beispielsweise Daten aus dem Melderegister, dem Zentralen Verkehrsinformationssystem (ZEVIS) oder dem Waffenregister, die durch gezielte Abfragen in die Analyse einbezogen werden können, soweit dies zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist. Abfragen in ZEVIS können zur Aufklärung des Sachverhalts beispielsweise erforderlich sein, wenn die Mobilität einer Anlassperson in Frage steht. Hat diese Person eine Waffenerlaubnis, kann darin ein gefahrerhöhendes Indiz gesehen werden. Die Funktionsweise der Analyseplattform stellt sicher, dass solche Informationen schnell zusammengeführt werden können.

Satz 2 erlaubt zudem eine ergänzende Einbeziehung von gesondert gespeicherten Datensätzen aus Internetquellen. Da gemäß Absatz 2 Satz 6 eine direkte Anbindung der Analyseplattform an Internetdienste unzulässig ist, dürfen diese Daten nicht

automatisiert einbezogen werden. Vielmehr müssen sie für jeden Analysevorgang händisch hinzugezogen werden.

Es handelt sich bei den nach Satz 2 einbezogenen Datensätzen regelmäßig um die aufbereiteten und bereits gefilterten Ergebnisse polizeilicher Recherchen. Voraussetzung ist, dass die Einbeziehung dieser Daten zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist.

Nach Absatz 3 Satz 3 dürfen Verkehrsdaten aus Funkzellenabfragen sowie Telekommunikationsdaten nicht in die automatisierte Datenanalyse einbezogen werden, wenn die Maßnahme gemäß Absatz 1 Nummer 3 bereits im Vorfeld einer konkretisierten Gefahr zur Anwendung kommt. Da bei der Verkehrsdatenerhebung aus Funkzellenabfragen insbesondere im Hinblick auf die Standortdaten häufig eine Vielzahl unbeteiligter Personen betroffen ist, führt der Ausschluss der Einbeziehung von Verkehrsdaten aus Funkzellenabfragen zu einer deutlichen Reduzierung der Eingriffsintensität. Dies dient sowohl dem Schutz unbeteiligter Personen als auch der Wahrung der Verhältnismäßigkeit. Darüber hinaus dürfen auch Telekommunikationsdaten nicht in die automatisierte Datenanalyse gemäß Absatz 1 Nummer 3 einbezogen werden, weil der zusätzliche Eingriff in das Fernmeldegeheimnis nach Artikel 10 Absatz 1 des Grundgesetzes – gerade im Hinblick auf die gegebenenfalls betroffenen Inhaltsdaten bei der Telekommunikation – eine Abstufung der Eingriffsintensität erforderlich macht. Im Vergleich zur konkretisierten Gefahr nach Absatz 1 Nummer 2 oder einer konkreten Gefahr nach Absatz 1 Nummer 1 zeichnet sich eine Maßnahme nach Absatz 1 Nummer 3 durch eine größere Ungewissheit sowohl in Bezug auf die Tatsachengrundlage als auch in Bezug auf den zum Schaden führenden Kausalverlauf aus. Dies erfordert eine entsprechende Begrenzung der Eingriffsintensität.

Nach Absatz 3 Satz 4 sind einzelfallbezogen auf der Analyseplattform gespeicherte Daten nach Satz 2 spätestens nach Ablauf von zwei Jahren zu löschen, soweit die weitere Speicherung der Daten nicht erforderlich ist. Diese Löschpflicht trägt zur Reduzierung der Datenmenge bei und wirkt somit eingriffsmildernd. Soweit mit der Einbeziehung von Verkehrsdaten, insbesondere den aus Funkzellenabfragen gewonnenen Daten, in dem für die automatisierte Datenanalyse bereitstehenden Datenpool eine bevorratende Speicherung von Verkehrsdaten möglich ist, müssen – so das Bundesverfassungsgericht – die erfassbaren Daten substantiell begrenzt und eine Höchstspeicherungsdauer geregelt sein (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 85). Die Löschfrist gilt nicht, soweit die weitere Speicherung der Daten nach Ablauf der Frist erforderlich ist. Die Möglichkeit, Daten über die Löschfrist

hinaus zu speichern, ist nach Satz 5 jedoch zeitlich begrenzt. Um den Anforderungen an Transparenz und aufsichtliche Kontrolle Rechnung zu tragen, ist die Entscheidung, die Löschfrist zu verlängern und die Daten weiter zu speichern, gemäß Satz 5 schriftlich zu begründen. Dem in Absatz 7 geregelten Anordnungsvorbehalt, der für alle Maßnahmen nach Absatz 1 gilt, wird auch bei der Entscheidung über die Verlängerung der Löschfrist Rechnung getragen.

Zur Verringerung der Eingriffsintensität der automatisierten Datenanalyse trägt schließlich bei, dass nach Absatz 3 Satz 6 personenbezogene Daten, die aus den besonders schwerwiegenden Grundrechtseingriffen der Wohnraumüberwachung und der Online-Durchsuchung stammen, nicht einbezogen werden dürfen.

Absatz 4 Satz 1 verweist auf eine entsprechende Geltung des § 15 Absatz 2 und 3 PolG. Damit wird sichergestellt, dass die weitere Nutzung der Daten im Rahmen der automatisierten Datenanalyse nach den Grundsätzen der Zweckbindung und Zweckänderung verfassungsrechtlich gerechtfertigt ist. Im Rahmen einer automatisierten Datenanalyse können personenbezogene Daten sowohl zweckwahrend als auch zweckändernd weiterverarbeitet werden. Eine zweckwahrende Nutzung von Daten kommt gem. § 15 Absatz 2 PolG nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich. Nicht erforderlich für eine weitere Nutzung der Daten im Rahmen der Zweckbindung ist das Vorliegen der für die Datenerhebung maßgeblichen Gefahrenlage. Ausreichend für eine weitere Nutzung der Daten ist vielmehr ein bloßer Spurenansatz. Etwas anderes gilt nur für Daten aus einer Wohnraumüberwachung oder Online-Durchsuchung, deren Weiterverarbeitung auf der Analyseplattform aber in Absatz 3 Satz 6 gesetzlich ausgeschlossen ist.

Nach § 15 Absatz 3 PolG dürfen Daten für einen anderen gefahrenabwehrrechtlichen Zweck genutzt werden, wenn die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Verhütung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Aus den Daten müssen sich im Einzelfall konkrete Ermittlungsansätze ergeben.

Ob Daten, die im Rahmen einer automatisierten Datenanalyse weiterverarbeitet werden, zweckwahrend oder zweckändernd verwendet werden, hängt maßgeblich von der Herkunft der Daten und den ursprünglichen Erhebungszwecken ab.

Zur praktischen Umsetzung des verfassungsrechtlichen Zweckbindungsgrundsatzes ist insbesondere eine Kennzeichnung der Daten erforderlich. Besonders schwierig ist dies bei einer automatisierten Einbindung von Dateien, zumal wenn es sich um große Datenbestände handelt. Eine begrenzende Wirkung gesetzlicher Zweckbindungsregelungen wird sich hier – so das Bundesverfassungsgericht – nur mittels organisatorischer und technischer Vorkehrungen realisieren lassen, die näher zu regeln sind, um das Eingriffsgewicht in verfassungsrechtlich anzuerkennender Weise reduzieren zu können (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 139). Technisch-organisatorische Vorkehrungen, die die Einhaltung der Zweckbindung sicherstellen, können etwa in der technischen Trennung von Datenbeständen nach unterschiedlichen Verarbeitungszwecken oder einer zweckabhängigen Verteilung von Zugriffsrechten auf Datenbestände bestehen (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 140).

Absatz 4 Satz 1 sieht deshalb vor, dass technisch-organisatorische Vorkehrungen insbesondere zur Einhaltung der Zweckbindung in einer Verwaltungsvorschrift zu regeln sind, die zu veröffentlichen ist. Das Bundesverfassungsgericht hat ausdrücklich darauf hingewiesen, dass der Gesetzgeber die Verwaltung verpflichten kann, die im Gesetz geregelten Vorgaben weiter zu konkretisieren, soweit die Vorgaben zu Art und Umfang der in die automatisierte Datenanalyse einbeziehbaren Daten und der zulässigen Verarbeitungsmethoden aus dem Gesetz selbst nur begrenzt erkennbar sind. Die Verwaltungsvorschrift muss aus Gründen der Transparenz und der Kontrolle veröffentlicht werden (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 113). Die Veröffentlichung erfolgt in dem für den Geschäftsbereich des Innenministeriums vorgesehenen amtlichen Bekanntmachungsblatt.

Absatz 4 Satz 2 regelt den wesentlichen Inhalt der Verwaltungsvorschrift, der in den Absätzen 5 und 6 näher konkretisiert wird. Der Absatz enthält Vorgaben zur Transparenz und Kontrolle (vgl. BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 109). Nach Satz 2 beinhaltet die Verwaltungsvorschrift ein Rollen- und Rechtekonzept, ein Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten, ein Konzept zur Zugriffskontrolle, das auch verdachtsunabhängige Stichprobenkontrollen der Zugriffe vorsieht, sowie nähere Bestimmungen über den Inhalt der erforderlichen Begründung nach Absatz 3 Satz 5 und Absatz 7 Satz 3.

Die Zugriffskontrolle nach Absatz 4 Satz 2 Nummer 3 wird durch die Protokollierung der einzelnen Arbeitsschritte gemäß § 74 PolG abgesichert. Auf diese Weise wird sichergestellt, dass nur berechtigte Personen eine automatisierte Datenanalyse

vornehmen können. Die gesetzlich vorgeschriebene Protokollierung sichert die nachträgliche aufsichtliche Kontrolle und ist gleichzeitig Voraussetzung für die Gewährleistung effektiven Rechtsschutzes gemäß Artikel 19 Absatz 4 GG. Als weiterer Kontrollmechanismus sind in der Verwaltungsvorschrift verdachtsunabhängige Stichprobenkontrollen durch die verantwortlichen Stellen zu implementieren.

Diesen Zwecken dient auch die nach Absatz 4 Satz 2 Nummer 4 näher auszugestaltende Begründungspflicht für die Anordnung der Verlängerung der Speicherfrist nach Absatz 3 Satz 5 sowie für die Anordnung einer automatisierten Datenanalyse nach Absatz 7 Satz 3. Gleichzeitig dient die Begründungspflicht auch der Selbstvergewisserung über die Rechtmäßigkeit der automatisierten Datenanalyse.

Übergeordnetes Ziel der Vorgaben in der Verwaltungsvorschrift ist es – wie sich aus Satz 3 ergibt –, die Datenbestände unter Berücksichtigung der in Absatz 1 beschriebenen Eingriffsschwellen auf das für den Analysezweck erforderliche Maß zu begrenzen und die Einbeziehung der Daten unbeteiligter Personen möglichst zu vermeiden.

Das Bundesverfassungsgericht hat mehrfach betont, dass eine Begrenzung von Art und Umfang der Daten und die zugelassene Methode der automatisierten Datenanalyse maßgeblichen Einfluss auf das Eingriffsgewicht und damit auf deren Zulässigkeit jeweils in Bezug auf die normierte Eingriffsschwelle haben (BVerfG, Urteil vom 16. Februar 2023, a.a.O., 76 ff., 90 ff.). Da die zugelassene Methode der automatisierten Datenanalyse bereits durch gesetzliche Vorgaben hinreichend begrenzt ist, dienen die mit der Verwaltungsvorschrift zu erlassenden Konkretisierungen in erster Linie dazu, die in die automatisierte Datenanalyse einzubeziehenden Datenbestände auf das für den Analysezweck erforderliche Maß zu begrenzen, die Umsetzung des Grundsatzes der Zweckbindung auch praktisch sicherzustellen und unbeteiligte Personen so weit wie möglich zu schützen.

Absatz 5 gibt vor, dass im Rollen- und Rechtekonzept nach Absatz 4 Satz 2 Nummer 1 festgelegt wird, wer innerhalb des Polizeivollzugsdienstes Zugriff auf welche Daten haben kann und mit welchen Rechten und Pflichten der Zugriff verbunden ist. Dabei sind die Zugriffsrechte nach dem Prinzip auszugestalten, dass die Zahl der Zugriffsberechtigten umso geringer ist, desto umfangreicher und sensibler die von der Zugriffsberechtigung umfassten Daten sind. Weil das Rollen- und Rechtekonzept an Rollen und nicht an Personen anknüpft, ist es möglich, dass eine Person mehrere

Rollen hat und deshalb über erweiterte Zugriffsrechte verfügt. Das Rollen- und Rechtekonzept führt damit zu einer Reduzierung des Umfangs der jeweils verarbeitbaren Daten und damit zu einer Verringerung der Eingriffsintensität.

Absatz 6 beschreibt das in der Verwaltungsvorschrift nach Absatz 4 Satz 2 Nummer 2 zu regelnde Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten, das ebenfalls zu einer Begrenzung des Datenbestandes und damit zu einer Verringerung der Eingriffsintensität beiträgt, indem entschieden wird, ob und in welcher Weise personenbezogene Daten verwendet werden dürfen. Grundlegend ist hier die Unterscheidung zwischen einerseits unbeteiligten und andererseits verurteilten, beschuldigten und verdächtigen Personen sowie sonstigen Anlasspersonen und deren Kontaktpersonen. Diese Unterscheidung ist für das Eingriffsgewicht der automatisierten Datenanalyse von maßgeblicher Bedeutung, denn das Eingriffsgewicht erhöht sich, wenn durch die automatisierte Datenanalyse Informationen über Personen erlangt werden, die objektiv in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den polizeilichen Eingriff durch ihr Verhalten nicht zurechenbar veranlasst haben (BVerfG, Urteil vom 16. Februar 2023, a.a.O., Rn. 77). Zum Schutz unbeteiligter Personen dürfen deren personenbezogene Vorgangsdaten grundsätzlich nicht in eine automatisierte Datenanalyse einbezogen werden.

Zur Verringerung der Eingriffsintensität führt schließlich auch, dass die Daten nach dem Gewicht des Grundrechtseingriffs bei der Datenerhebung so kategorisiert werden müssen, dass deren eingeschränkter oder ausgeschlossener Verwendbarkeit bei schwerwiegenden Grundrechtseingriffen Rechnung getragen wird. Wegen der besonderen Eingriffsintensität von Wohnraumüberwachungen und Online-Durchsuchungen ist in Absatz 3 Satz 6 bereits gesetzlich ausgeschlossen, dass die aus solchen Maßnahmen erlangten Informationen in die automatisierte Datenanalyse einbezogen werden. Bei Daten, die aus anderen grundrechtsintensiven Eingriffen erlangt wurden, kommt eine Weiterverarbeitung der Daten nach den Grundsätzen der Zweckbindung nur in Betracht, wenn die Voraussetzungen des § 15 Absatz 2 oder 3 PolG vorliegen.

Durch die zu treffenden technisch-organisatorischen Vorkehrungen muss sichergestellt werden, dass die Grundsätze der Zweckbindung auch tatsächlich umgesetzt werden.

Absatz 7 dient der verfahrensmäßigen Absicherung, indem er Maßnahmen nach Absatz 1 auch einem Anordnungsvorbehalt unterwirft. Er trägt zugleich dem hohen

Eingriffsgewicht einer automatisierten Datenanalyse in das Recht auf informationelle Selbstbestimmung Rechnung. Die Anordnung ist durch die Leitung eines regionalen Polizeipräsidiums, des Polizeipräsidiums Einsatz oder des Landeskriminalamts schriftlich zu erteilen und zu begründen. Sie bezieht sich auf den Einsatz der automatisierten Datenanalyse in einem konkreten Gefährdungssachverhalt in seiner Gesamtheit und muss daher nicht für jeden einzelnen Suchvorgang im Rahmen dieses Sachverhalts neu angeordnet bzw. bestätigt werden. Dies sichert die vom Bundesverfassungsgericht geforderte aufsichtliche Kontrolle, die ein Ausfluss aus dem Verhältnismäßigkeitsgrundsatz darstellt. Für eine effektive Kontrolle ist dabei unerlässlich, dass eigenständig ausformulierte Begründungen dafür gegeben werden, warum bestimmte Datenbestände zur Gefahrenabwehr oder Verhütung bestimmter Straftaten im Wege automatisierter Anwendung analysiert werden. Eine Delegation der Anordnungsbefugnis ist bei Gefahr in Verzug auf besonders beauftragte Beamte möglich.

Nach Absatz 8 ist vor der Einrichtung oder einer wesentlichen Änderung einer Analyseplattform nach Absatz 1 die Landesbeauftragte oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit anzuhören. Die Regelung gewährleistet eine effektive und unabhängige datenschutzrechtliche und aufsichtliche Kontrolle.

Davon unbenommen gelten die allgemeinen datenschutzrechtlichen und aufsichtlichen Regelungen des Polizeigesetzes.

Zu Nummer 3:

Der neue § 57a schafft eine ausdrückliche Rechtsgrundlage für die Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von informationstechnischen Produkten einschließlich KI-Systemen und KI-Modellen im Sinne der KI-VO durch die Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst anhand von Echtdaten. Informationstechnische Produkte sind entsprechend der Legaldefinition in § 2 Absatz 9a des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten. Zu den informationstechnischen Produkten zählen insbesondere auch KI-Systeme, also maschinengestütze Systeme, die für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt sind und die nach ihrer Betriebsaufnahme anpassungsfähig sein können und aus den erhaltenen Eingaben für explizite oder implizite Ziele ableiten, wie Ausgaben - wie etwa Vorhersagen,

Inhalte, Empfehlungen oder Entscheidungen - erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können (KI-Systeme gem. Art. 3 Nr. 1 VO KI-VO) sowie diesen Systemen zugrundeliegende KI-Modelle mit oder ohne allgemeinen Verwendungszweck i.S.d. der KI-VO.

Erfüllt das Testen und Training von informationstechnischen Produkten einschließlich KI-Systemen und KI-Modellen im Sinne der KI-VO im Einzelfall die für die wissenschaftliche Forschung kennzeichnenden Merkmale, ist § 57 als Rechtsgrundlage für die Datenverarbeitung heranzuziehen.

Eine Verarbeitung personenbezogener Daten durch die Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst nach § 57a Absatz 1 Satz 1 ist ausschließlich zum Zwecke der Entwicklung, des Trainings, des Testens, der Validierung und der Beobachtung von informationstechnischen Produkten einschließlich KI-Systemen und KI-Modellen im Sinne der KI-VO zulässig. Zudem muss es sich um informationstechnische Produkte handeln, die die Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst für die polizeiliche Aufgabenwahrnehmung entwickeln oder nutzen wollen. Die Datenverarbeitung muss zur Erreichung der benannten Zwecke erforderlich sein. Insbesondere muss eine Erforderlichkeit für unveränderte Daten bestehen oder eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich sein. Die Erforderlichkeit der Verarbeitung unveränderter Daten bildet hierbei keinen Sonderfall der unmöglichen oder nur mit unverhältnismäßigem Aufwand möglichen Anonymisierung oder Pseudonymisierung. Es handelt sich vielmehr um eine alternative Ermächtigung für die Fälle, in denen eine Anonymisierung oder Pseudonymisierung zwar objektiv möglich und auch mit verhältnismäßigem Aufwand durchführbar, aber praktisch nicht zielführend wäre, da sie den Erkenntniswert oder die Funktionstauglichkeit des betreffenden informationstechnischen Produktes erheblich beeinträchtigen würde. Insbesondere im Bereich der Evaluation und Validierung von KI-Systemen dürfte der Einsatz von realitätsnahen, also unveränderten, Testdaten in vielen Fällen erforderlich sein. Eine Anonymisierung oder Pseudonymisierung könnte in diesen Fällen den entscheidenden Kontext oder die technische Struktur, welche das System lernen oder prüfen soll, entwerten.

Die Regelungen in Absatz 1 Sätze 2 und 3 stellen eine gesetzliche Sicherung vor den spezifischen Risiken selbstlernender Systeme dar und verpflichten zu technisch-organisatorischen Maßnahmen beim Testen dieser Systeme. Inbesondere beim Einsatz von Techniken, bei denen KI-Modelle mit Daten trainiert werden, besteht die

Gefahr, dass darauf aufbauende Systeme Diskriminierungen fortschreiben oder verstärken, wenn unvollständige, fehlerhafte oder nicht repräsentative Trainingsdaten verwendet werden oder auch wenn die Datenausgaben die Eingaben für künftige Operationen beeinflussen (Rückkopplungsschleifen). Es muss also unter anderem sichergestellt werden, dass die Trainings-, Validierungs- und Testdatensätze im Hinblick auf die Zweckbestimmung relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig sind.

Absatz 1 Satz 4 sowie die Absätze 2 und 3 entsprechen Regelungen in § 57 Absatz 1 Satz 2, Absätze 2 und 4. Es handelt sich um Schutzregelungen zur zweckkonformen Datenverarbeitung.

Zu Nummer 4:

Mit den Folgeänderungen in § 74 wird die nach der Rechtsprechung des Bundesverfassungsgerichtes erforderliche Protokollierung von Verarbeitungsvorgängen bezüglich solcher Daten, die aus verdeckten beziehungsweise eingriffsintensiven Maßnahmen gewonnen werden, auf die Einführung der automatisierten Datenanalyse erstreckt. Absatz 1 bestimmt die Angaben, auf die sich jede Protokollierung bei den genannten verdeckten und eingriffsintensiven Maßnahmen zu erstrecken hat. In der neuen Nummer 1 des Absatzes 2 werden weitere, für die automatisierte Datenanalyse zu protokollierende Angaben und insbesondere die zu protokollierenden Personen festgelegt.

Zu Nummer 5:

Mit den Folgeänderungen in § 86 wird die nach Artikel 13 Absatz 2 der Richtlinie (EU) 2016/680 und nach der Rechtsprechung des Bundesverfassungsgerichts vorgegebene Informationspflicht auf die betroffene Person erstreckt, soweit gegen diese nach einer automatisierten Datenanalyse weitere polizeiliche Maßnahmen getroffen werden.

Zu Nummer 6:

Der neu gefasste § 90 Absatz 1 ersetzt die bisher bestehende Berichtspflicht gegenüber dem Landtag durch eine Unterrichtung des Parlamentarischen Kontrollgremiums. Diese Unterrichtung wird auch auf die automatisierte Datenanalyse nach § 47a ersteckt. Im Rahmen der Unterrichtung ist darzustellen, in welchem Umfang von den aufgeführten Maßnahmen aus Anlass welcher Art von

Gefahrenlagen Gebrauch gemacht wurde und betroffene Personen benachrichtigt wurden. Damit wird den Anforderungen des Bundesverfassungsgerichts in seinem Urteil zum BKA-Gesetz (Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 142ff.) Rechnung getragen.

Absatz 2 normiert die vom Bundesverfassungsgericht ebenfalls geforderte Pflicht zur Unterrichtung der Öffentlichkeit und sieht insoweit ein jährliches Intervall vor.

Zu Nummer 7:

Mit den Folgeänderungen in § 98 werden die in Umsetzung des Artikels 46 der Richtlinie (EU) 2016/680 festgelegten Aufgaben der Aufsichtsbehörde für den Datenschutz auf die automatisierte Datenanalyse erstreckt.

Zu Nummer 8:

Mit der Folgeänderung in § 130 wird die Verordnungsermächtigung für die Übertragung der Anordnungsbefugnis auf die automatisierte Datenanalyse erstreckt.

Zu Artikel 2 - Änderung der Verordnung zur Durchführung des Polizeigesetzes (DVO PolG):

Mit dem neuen Absatz 3 wird von der Verordnungsermächtigung des § 130 PolG Gebrauch gemacht. Die Anordnungsbefugnis nach § 47a Absatz 7 PolG kann bei Gefahr in Verzug bei den regionalen Polizeipräsidien auf die Leitung des Führungs- und Einsatzstabes, die Leitung der Schutzpolizeidirektion und die Leitung der Kriminalpolizeidirektion sowie auf den Polizeiführer vom Dienst delegiert werden. Im Landeskriminalamt kann sie auf die Abteilungsleitungen sowie auf den Polizeiführer vom Dienst delegiert werden.

Zu Artikel 3 - Inkrafttreten

Die Vorschrift regelt das Inkrafttreten des Gesetzes.