Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit

Der Landesbeauftragte fur den Datenschutz und die Informationsfreiheit
Baden-Wurttemberg | Postfach 10 29 32 | 70025 Stuttgart

Ministerium des Inneren, fur Digitalisierung und Kommunen Baden-Wurttemberg

Per E-Mail

Name [redacted]
Telefon +49 711 615541-[redacted]
E-Mail poststelle@lfdi bwl de

Geschaftszeichen LfDI[redacted]
(bei Antwort bitte angeben)

Datum 05 06 2025

Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften

Hier. Stellungnahme zum neuen Entwurf aus Ihrem Schreiben vom 22. Mai 2025
Ihr Zeichen: [redacted]

Sehr geehrte Damen und Herren,

wir danken für die Einbindung und nehmen wie folgt Stellung:

A. Zu § 45a PolG-E

Wir haben keine erganzenden Anmerkungen gegenuber unserer Stellungnahme vom 27 März 2025.

B. Zu § 47a PolG-E

Mit Blick auf die Erheblichkeit der Regelung und die komplexe Rechts- und Sachlage nehmen wir gerne die erneute Moglichkeit zur Stellungnahme wahr, um zunächst einige grundsatzliche Erwägungen mitzuteilen und anschließend auf einzelne Aspekte näher einzugehen.

Die Regelung setzt bereits eine Vielzahl an Voraussetzungen um, die vom Bundesverfassungsgericht in seinem Urteil vom 16 2.2023 – 1 BvR 1547/19, 1 BvR 2634/20 vorgegeben wurden. Gleichwohl sind wir nach naherer Prüfung zu dem Ergebnis gekommen, dass vor dem Hintergrund der umfassenden Weichenstellung für die Zukunft polizeilicher Arbeit und umfangreichen Datenverarbeitung einige Aspekte klarer durch den Gesetzgeber geregelt werden sollten, bzw.

müssen, letzteres insbesondere mit Blick auf die nunmehr eingefügte Erlaubnis für eine automatisierte Bewertung der Daten mittels Künstlicher Intelligenz. Diese wird unseres Erachtens verfassungsrechtlichen Anforderungen nicht gerecht (dazu Näheres s.u. II 3.)

I. Grundsätzliches

Die Einführung einer Regelung zur automatisierten Datenanalyse, nunmehr avisiert unter Einbeziehung der Möglichkeiten von Künstlicher Intelligenz, stellt für die polizeiliche Arbeit einen grundlegenden Wandel dar. Sie birgt erhebliche Potentiale für die Effizienz polizeilichen Handelns und damit für die Sicherheit in Baden-Württemberg. Die Bewältigung großer Datenmengen ist heute wesentlicher Bestandteil polizeilicher Arbeit und bedarf dringend eines adäquaten rechtlichen Rahmens. Gleichzeitig handelt es sich bei einer automatisierten Analyse großer Datenmengen um ein mächtiges Instrument, welches erheblich in die Grundrechte der Personen eingreift, über die Informationen bei der Polizei vorhanden sind, bzw durch diese verfügbar gemacht werden können (präziser zu Art und Umfang der Daten, die in die Analyse einfließen können, s.u. II. 3). Das Bundesverfassungsgericht hat in seinem Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20 bereits darüber entschieden, dass eine automatisierte Datenanalyse mit dem Grundgesetz vereinbar sein kann Vor diesem Hintergrund stellen wir nicht in Abrede, dass der Gesetzgeber der Exekutive diese Maßnahme erlauben darf. Auch kommt dem Gesetzgeber eine Einschätzungsprärogative zu Er verfügt also bei der Normsetzung über einen in Teilen der Kontrolle entzogenen Spielraum bei der Beurteilung der tatsächlichen Lage und den Folgen seiner Normsetzung. Allerdings wirft der derzeitige Entwurf Fragen in Bezug darauf auf, ob der Gesetzgeber durch ihn in hinreichender Weise (selbst) über die Eingriffe in die Rechte und Freiheiten betroffener Personen entscheidet Gerade weil die Sach- und Rechtslage zur automatisierten Datenanalyse komplex ist, müssen unseres Erachtens wesentliche Faktoren durch den Gesetzgeber klarer und deutlicher entschieden und begründet werden.

Auch wenn das Bundesverfassungsgericht die Verknüpfung und Auswertung polizeilicher Datenbestände für grundsätzlich grundgesetzkonform erachtet und dabei auch die Möglichkeit gesehen hat, Teile der Regelung in eine Verwaltungsvorschrift zu verlegen, so bleibt es dennoch dabei, dass die Entscheidung über dasjenige, was „für die Grundrechtsverwirklichung wesentlich“ ist, durch den Gesetzgeber entschieden werden muss (s. z.B. BVerfG, Beschluss vom 8 8. 1978 - 2 BvL 8/77). Je wesentlicher eine Angelegenheit für den Bürger und die Allgemeinheit ist, desto höhere Anforderungen werden an den Gesetzgeber gestellt. Je nachhaltiger also die Grundrechte Einzelner durch eine Regelung betroffen oder je gewichtiger die Auswirkungen für die Allgemeinheit sind, desto präziser und enger muss die gesetzliche Regelung sein. Mit der

Einfuhrung der Datenanalyse wird durch die Zusammenführung einer Vielzahl an „Datentöpfen" das Eingriffsgewicht für den Einzelnen deutlich erhoht, denn auf diese Weise lassen sich viel umfangreichere Informationen zusammentragen, gar Profile über einzelne Personen anlegen, da umfassende Einblicke in Gewohnheiten, soziale Verankerungen, etc. möglich werden – also ein Bewegungs- oder Verhaltensprofil einer Person oder ein umfassenderes Personlichkeitsbild geschaffen werden kann (vgl BVerfG, Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, Rn 77). Darüber hinaus ist erwartbar, dass die Einführung der Analysemoglichkeit Auswirkungen auf die Allgemeinheit und deren Erleben ihrer Freiheit haben wird. Beides wird durch die Erganzung um den Einsatz „Kunstlicher Intelligenz" verstarkt.

Wir mochten zunachst darauf hinweisen, dass die technische Grundkonzeption der Datenanalyse zu einer Risikoerhohung für betroffene Personen fuhrt, die nicht in einer rechtlichen Notwendigkeit gründet. Dem Grunde nach ist die automatisierte Datenanalyse eine Dateisystemübergreifende Suchfunktion mit Visualisierungseffekten (so auch in der Begrundung. *Zunächst soll eine Rechtsgrundlage dafür geschaffen werden, bisher unverbundene Daten und Datenquellen des Polizeivollzugsdienstes in einer Analyseplattform zusammenzuführen, um die vorhandenen Datenbestande durch Suchfunktionen systematisch erschließen zu können (automatisierte Datenanalyse)* ". Dass diese Suchfunktion aktuell eine Kopie samtlicher Datenbestande erfordert, ist der zersplitterten polizeilichen IT-Infrastruktur geschuldet, in der die vorhandenen Daten nicht gleichzeitig durchsucht werden können. Klar ist also, dass die Kopie der vorgesehenen Datenbestande nur deshalb zur gemeinsamen Durchsuchung erforderlich ist, weil bei den vorhandenen Systemen technisch keine hinreichende fachverfahrenübergreifende Durchsuchung möglich ist. Dieser Umstand grundet folglich nicht in einer rechtlich notwendigen Trennung bestimmter Daten, sondern in der Art und Weise der technischen Konzeption polizeilicher Datenverarbeitung. Mit der Regelung wird folglich mindestens ein Verarbeitungsvorgang geschaffen – die Zusammenführung der genannten Datentöpfe – der nur deshalb notwendig wird, weil die vorhandenen Verarbeitungssysteme technisch inkompatibel sind Allein durch die Doppelspeicherung entsteht fur die Personen, um deren Daten es dabei geht, ein hoheres Risiko. Auch wenn alle erdenklichen Schutzmaßnahmen technischer und organisatorischer Art für diese Daten ergriffen werden, so ist jede Schutzmaßnahme eine Wahrscheinlichkeitsrechnung und keine absolute Sicherheit

Das Recht auf Informationelle Selbstbestimmung darf durch eine gesetzliche Grundlage eingeschrankt werden, wenn die Regelung verhältnismaßig ist und sich aus ihr die Voraussetzungen und der Umfang der Beschränkungen klar und für den Burger erkennbar ergibt und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (BVerfG, Urteil vom 15. Dezember

1983 – 1 BvR 209/83, Rn. 149) Je tiefer der Eingriff, desto mehr muss der Gesetzgeber auch organisatorische und verfahrensrechtliche Vorkehrungen treffen, um die Rechte und Freiheiten betroffener Personen zu schutzen (vgl. oben). Das Bundesverfassungsgericht hat in seinem Urteil vom 16.2 2023 – 1 BvR 1547/19, 1 BvR 2634/20 u.a. auf die folgenden Aspekte verwiesen, die bei der Abwägung des Eingriffs durch eine automatisierte Datenanalyse zu berucksichtigen – und dementsprechend im Wesentlichen durch den Gesetzgeber zu entscheiden – sind · die Art der betroffenen Daten, den Umfang der Daten, die Methode der Datenverarbeitung (und mögliche Ergebnisse), die Eingriffsschwellen, die Abmilderung der Eingriffe und die Folgen der zu erlaubenden Eingriffe.

Anders als in der Datenschutz-Grundverordnung enthalt die RL (EU) 2016/680, die die Verarbeitung personenbezogener Daten zu polizeilichen Zwecken regelt, keinen ausdrücklichen Grundsatz der Transparenz. Aufklarungs- und Auskunftspflichten als Schutzvorkehrung fur betroffene Personen sind jedoch auch dem Verfassungsrecht immanent (vgl z B. BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83, Rn. 154). Bei heimlichen Maßnahmen, bei denen die Erlangung von Rechtsschutz erschwert ist, gilt dies umso mehr

II. Einzelnes

1. Zu den Eingriffsschwellen

In der Gesetzesbegründung heißt es zum Zweck der Einfuhrung einer Datenanalyse· *„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.“*. Dass dem so ist, wollen wir selbstverstandlich nicht bestreiten. Allerdings sieht § 47a PolG die Analyse in einer Vielzahl an weiteren Konstellationen vor, z B läge eine konkrete Gefahr fur den Leib einer Person (vgl. Eingriffsschwelle aus § 47a Abs. 1 Nr. 1 PolG-E) auch im Falle einer hinreichend wahrscheinlichen Schlägerei oder leichten Körperverletzung vor. Zwar heißt es in der Regelung, dass der Einsatz der Analyse nur dann zulässig ist, wenn die Analyse *erforderlich* ist, um die Gefahr abzuwehren. Aus Sorge vor einer zu weitreichenden Auslegung dieses Begriffs und der Unmöglichkeit vorgelagerten sowie eingegrenztem nachträglichen Rechtschutzes (Näheres s.u. II. 4) empfehlen wir mindestens die Darlegung dessen, was „erforderlich“ meint. Derzeit wird in der Gesetzesbegründung nur auf die Voraussetzung einer konkreten Gefahr eingegangen und geschildert, dass die Eingriffsschwelle an enge Voraussetzung geknüpft ist, „wie sie allgemein für eingriffsintensive Maßnahmen gelten“ Dass allerdings die Erforderlichkeit – insbesondere

bei europarechtskonformer Auslegung im Lichte der JI-RL (vgl hierzu auch EuGH ECLI:EU:C.2022:491, Rn 148, 149) – eine weitere Eingrenzung enthält, geht daraus nicht hervor. Deswegen empfehlen wir mindestens in der Gesetzesbegründung aufzugreifen, dass bei der Erforderlichkeit strenge Maßstabe anzusetzen sind. Klar muss sein, dass die automatisierte Datenanalyse ein Instrument ist, dass nur dann zum Einsatz kommt, wenn es um erhebliche Gefahren geht und andere Mittel nicht zur Verfügung stehen.

2. Zu „Art und Umfang" der verwendeten Daten:

Mit Blick auf die Wesentlichkeitstheorie, den Bestimmtheitsgrundsatz und die Normenklarheit ist bedenklich, dass die Bestimmung der in die Analyse einzuspeisenden Inhalte nicht an den grundgesetzlich geschutzten Inhalten (d h. an den Informationen uber die naturlichen Personen) orientiert ist, sondern daran, wie die polizeilichen Arbeitssysteme strukturiert sind. Denn damit fallt der Gesetzgeber keine klare Entscheidung darüber, *welche* Informationen uber *welche* und *wie viele* Personen verarbeitet werden durfen. Diese Entscheidung fallt infolge dieser Konzeption weitestgehend die Exekutive, indem sie entscheidet, welche Daten in die jeweiligen Systeme eingespeist werden. Dies begegnet insbesondere mit Blick auf die sog „Vorgangsdaten" und „Falldaten" Bedenken.

Vorgangsdaten meint diejenigen Daten, die im Vorgangsbearbeitungssystem der Polizei gespeichert sind. Sie dienen der Aufgabenerfullung sowie der Vorgangsbearbeitung und Dokumentation repressiven oder präventiven polizeilichen Handelns. Das bedeutet, dass sich darin Informationen zu strafrechtlichen Ermittlungen befinden, beispielsweise zu einem Raububerfall, aber auch zu Ruhestorungen, Verkehrsunfällen oder Versammlungen. Hier konnen folglich auch personenbezogene Daten beispielsweise von Versammlungsleiter_innen, Rettungskräften, Hinweisgeber_innen oder sonstigen Personen enthalten sein, die selbst keinen Anlass im polizei- oder strafrechtlichen Sinne gegeben haben, um in polizeilichen Informationssystemen aufzutauchen (gemeint: als Verdachtige oder Verantwortliche („Störer")) Inwieweit bereits jetzt innerhalb des Vorgangsbearbeitungssystems eine Kennzeichnung dieser Daten geschieht und eine Vorsortierung der Inhalte möglich ist, ist uns nicht bekannt. Jedenfalls ist in § 47a PolG-E derzeit keine Differenzierung *der Inhalte* der personenbezogenen Daten auf Ebene des Gesetzes vorgesehen. Wessen Daten einbezogen und wie sie unterschieden würden, soll stattdessen in der Verwaltungsvorschrift festgelegt werden, s § 47a Abs 6 Pol-E: *„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, verdachtigen und sonstigen Anlasspersonen sowie deren Kontaktpersonen und*

andererseits unbeteiligten Personen. Zum Schutz unbeteiligter Personen werden deren personenbezogene Vorgangsdaten in eine automatisierte Datenanalyse nicht einbezogen ". Damit wird ein entscheidender Aspekt der Tragweite des Grundrechtseingriffs in die Hande der Exekutive gelegt und der öffentlichen parlamentarischen Debatte entzogen. Trotz Verstandnisses für das polizeiliche Interesse, moglichst viele Daten in die Auswertung einzubeziehen, die ggf. auch Verbindungen zwischen Personen durch Dritte ermoglichen, begegnet es zumindest Bedenken, dass nach der vorgesehenen Regelung nicht der Gesetzgeber, sondern die Exekutive darüber entscheidet, wessen Daten zur Analyse freigegeben werden und in welchem Umfang.

Darüber hinaus gilt der vorgesehene Ausschluss Unbeteiligter nach derzeitiger Formulierung nur für Vorgangsdaten. Fur alle anderen „Datentopfe" ist kein Ausschluss vorgesehen Dies ist insbesondere mit Blick auf Falldaten problematisch. Denn auch diese konnen eine Vielzahl verschiedenster Informationen enthalten, sollen sie es doch gerade ermöglichen, Strukturen und Beziehungsnetzwerke zu ermitteln und abzubilden. Es ist daher nicht verständlich weshalb der Ausschluss „Unbeteiligter" – mag der Begriff auch rechtsunsicher sein – nur für Vorgangsdaten gelten soll. So konnen Personen, die nur zufallig in Kontakt mit der Polizei gekommen sind, in allen Bereichen auftreten. Es ist nicht nachvollziehbar – und aus der Gesetzesbegründung heraus auch nicht ersichtlich – aus welchem Grund es angemessen sein sollte, die Daten Unbeteiligter uberhaupt in die Analyse miteinzubeziehen Dies insbesondere vor dem Hintergrund, dass polizeiliche Daten nach § 72 PolG bereits jetzt zu kennzeichnen sind. Spätestens mit Ablauf der Ubergangsfrist zur Umsetzung der Kennzeichnungspflicht besteht kein Grund, die vorhandene Kennzeichnung aus allen Systemen zum Schutz betroffener Personen einzusetzen und über die Vorgangsdaten hinaus gesetzlich vorzuschreiben

Wir begrüßen ausdrucklich, dass personenbezogene Daten, die aus einer Wohnraumüberwachung oder einer Online-Durchsuchung gewonnen wurden, nicht in die automatisierte Datenanalyse einbezogen werden durfen Nicht ausgeschlossen sind allerdings beispielsweise Informationen, die aus dem Einsatz verdeckter Ermittler, längerfristige Observationen oder der Einsatz technischer Mittel außerhalb von Wohnungen gewonnen wurden. Auch in diesen Fallen sind voraussichtlich eine Vielzahl an Personen miterfasst, die keinen eigenen Anlass gesetzt haben (wieder· als Verdachtige im straf- oder Verantwortliche im polizeirechtlichen Sinne).

Wir weisen auch darauf hin, dass polizeiliche Daten grundsätzlich dahingehend zu trennen sind, welche zum Zwecke der Strafverfolgung verarbeitet werden und welche zum Zwecke der Gefahrenabwehr Diese rechtlich vorgeschriebene Trennung ist in der polizeilichen Arbeit oft schwierig umzusetzen. Bei der Konzeption, welche strafprozessualen Daten in die Analyse einfließen dür-

fen, müssen demnach die §§ 481 ff. StPO berücksichtigt werden. § 49 BDSG kann unserer Auffassung nach nicht herangezogen werden, soweit die StPO bereits spezielle Regelungen zur Weiterverarbeitung trifft.

3. Zum Einsatz künstlicher Intelligenz

Aus verfassungsrechtlicher Perspektive ist der Einsatz von „Künstlicher Intelligenz" eine besondere Art der automatisierten Datenverarbeitung Mit Blick auf die o g. dargelegten Grundsätze, dass der Gesetzgeber die für die Grundrechtsverwirklichung wesentlichen Aspekte selbst entscheiden muss, begegnet die hier angestrebte Regelung erheblichen Bedenken. Es bleibt unklar, welche Arten von Kunstlicher Intelligenz eingesetzt werden sollen und welchem Zweck sie dienen (vgl. Kriterium des BVerfG in Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20 oben „Methoden" der Datenverarbeitung). Die Gesetzesbegründung nennt hier zwar einige Beispiele, die unseres Erachtens allerdings zu vage bleiben. Die aktuelle Formulierung im Wortlaut enthalt eine Pauschalerlaubnis, die durch diese Beispiele nicht eingegrenzt wird

In der Pauschalitat der Norm bleibt unklar, was genau und weshalb der Gesetzgeber den Einsatz von Kunstlicher Intelligenz bei der Datenanalyse zulassen möchte. Trotz Einschatzungsprärogative ist dies jedoch entscheidender Ausgangspunkt von Gesetzgebung· Zu welchem Zweck, mit welchem *Ziel,* und mit welchem Mittel soll der Eingriff in ein Grundrecht erlaubt werden. Eben dies ergibt sich nicht aus dem Wortlaut des Regelungsentwurfs („bewerten") und auch die Gesetzesbegründung fuhrt nur Beispiele an, lässt somit potentiell Raum für nicht uberblickbare und zukünftige technische Möglichkeiten Die Grenzen der Eingriffsbefugnis müssen jedoch durch den Gesetzgeber festgelegt werden, insbesondere mit Blick auf den Zweckbindungsgrundsatz. Grundsätzlich wird nicht in Abrede gestellt, dass der Gesetzgeber automatisierte Datenverarbeitungen, die als KI qualifiziert werden konnen, erlauben darf. Allerdings muss klar sein, welche Bewertungen mittels KI erlaubt werden sollen. Dies bleibt im vorliegenden Entwurf jedoch offen.

4. Zur Transparenz für die betroffenen Personen und Kontrollmechanismen als Faktoren zur Abmilderung der Eingriffsintensität

Im derzeitigen Entwurf ist eine Benachrichtigung im Sinne des § 86 PolG nur für diejenigen Personen vorgesehen, „gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden".

Was unter „weitere Maßnahmen" zu verstehen ist, bleibt in der Formulierung des § 86 PolG-E mit Blick auf den Bestimmtheitsgrundsatz zu unbestimmt. So könnten einerseits „Standardmaßnah-

men" der Polizei darunterfallen. Andererseits konnte als Maßnahme auch jeder weitere Grundrechtseingriff verstanden werden, so z. B. das Extrahieren von der Analyseplattform und Einfugen in einen anderen Kontext, beispielsweise ein Fallbearbeitungssystem, ein Vorgangsbearbeitungssystem oder – je nach Konzeption der Analyseplattform – das dortige Abspeichern als vorgangsrelevant o.A. mit der Konsequenz, dass eine Benachrichtigungspflicht ausgelost würde.

Eine vorgelagerte Kontrolle, wie sie durch das Anordnungserfordernis in § 47a Absatz 7 PolG-E vorgesehen ist, wird nach unserer Bewertung durch die Delegationsmoglichkeit in § 4 DVO PolG-E zu weit aufgeweicht. Zwar kann nachvollzogen werden, dass beispielsweise am Wochenende eine Notwendigkeit bestehen kann, dass auch ein Polizeifuhrer vom Dienst eine automatisierte Datenanalyse anordnen kann, allerdings schränkt die derzeitige Formulierung die Delegationsmöglichkeit nicht auf Notfälle oder Situationen ein, in denen die jeweiligen Leitungen nicht erreichbar sind. Der Gesetz-, bzw. in § 4 DVO-PolG der Verordnungsgeber, erlaubt demnach die Delegation an den Polizeifuhrer vom Dienst ohne dies an weitere Voraussetzungen zu knüpfen. Auch konnte es Rechtsunsicherheit begegnen, was genau von dem Anordnungserfordernis erfasst ist, namentlich, was mit „Maßnahme" in Absatz 7 gemeint ist. So ließe sich der Wortlaut derart auslegen, dass jeder einzelne Suchvorgang auf der Analyseplattform einer Anordnung bedarf

5. Zu den noch zu regelnden technischen und organisatorischen Vorkehrungen

Die Regelungen zum Rechte- und Rollenkonzept müssen selbstverständlich die bestehenden Rechte- und Rollenkonzepte konsolidieren und keine faktische Umgehung zu trennender Datensätze erlauben Hier verweisen wir nochmals auf §§ 481 ff. StPO. Soweit die Kategorisierung und Kennzeichnung neue Informationen uber Personen kreiert muss klar sein, dass die Vorschrift keine Erlaubnis zur Kategorisierung von Personen enthält.

C. Zu § 57 a PolG-E

Wir begrußen die Schaffung einer ausdrücklichen Rechtsgrundlage zur Testung von polizeirelevanter IT-Produkte Auf diese Weise kann rechtssicher und praxistauglich geprüft werden, welche Produkte sich für die polizeiliche Arbeit eignen. Insbesondere mit Blick auf die digitale Souveränitat befurworten wir auch die Möglichkeit fur staatliche Stellen, selbst Anwendungen herzustellen und auf die eigenen Bedürfnisse zuschneiden zu konnen. Dies gilt auch fur solche, die Künstliche Intelligenz einbeziehen.

Ausweislich der Ausfuhrungen unter „I. Zielsetzung" der Gesetzesbegründung soll die Regelung sowohl fur KI-gestützte, als auch fur nicht KI-gestützte IT-Produkte gelten In der Begrundung

zu § 57a PolG-E wird Kunstliche Intelligenz jedoch nicht erwahnt Die zu Beginn verwendete Formulierung. „Damit IT- und KI-Systeme ordnungsgemäß getestet und trainiert werden können [ ]", suggeriert darüber hinaus eine Unterscheidung zwischen „IT-Systemen" und „KI-Systemen" – was dem unter „Zielsetzung" formulierten Wunsch jedoch zuwiderlaufen würde Da der Wortlaut der Norm selbst nur „IT-Produkte" benennt, waren so KI-basierte Produkte wohl nicht von der Regelung erfasst Diese Unklarheit sollte behoben werden. Es ist allerdings wichtig zu betonen, dass KI-Tools nicht ausschließlich als IT-Produkt betrachtet werden konnen. Eine pauschale Einordnung als einfaches IT-Produkt ist nicht sachgerecht, insbesondere sollten Schnittmengen mit der KI-VO geprüft werden.

Wir empfehlen zu prüfen, ob eine Trennung zwischen einer Rechtsgrundlage fur die Testung von KI-gestutzten IT-Produkten und nicht KI-gestutzten IT-Produkten grundsätzlich aus Grunden der Normenklarheit sinnvoll ist. Denn mit Blick auf die KI-VO könnte Rechtsunsicherheit durch die Verwendung nicht deckungsgleicher Begriffe entstehen. Beispielsweise wurde im Rahmen der Novellierung des LDSG in § 11 a LDSG-E wie folgt für die Erlaubnis von KI-Training formuliert: „Für die Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von KI-Systemen und KI-Modellen [..]". In § 57a PolG-E wird hingegen im Wortlaut erlaubt, „vorhandene personenbezogene Daten zur Entwicklung, Uberprüfung, Anderung oder zum Trainieren von IT-Produkten weiter[zu]verarbeiten". Die divergierenden Wortlaute sollten miteinander und der KI-VO kohärent sein, um Rechtsunsicherheit vorzubeugen

Wir begrüßen, dass die Problematik diskriminierender Algorithmen ausdrucklich in der Regelung aufgegriffen wird.

Nicht nachvollzogen werden kann die Unterscheidung zwischen Nr. 1 und Nr 2 des Absatzes 1 Halbsatz 2. Denn Nr. 2 unterscheidet bereits zwischen der Un*moglichkeit* und der Un*verhältnismaßigkeit* einer Anonymisierung/ Pseudonymisierung Und eine Unverhältnismäßigkeit setzt bereits voraus, dass die Echtdaten benotigt werden. Durch die alternative Auflistung („oder") werden die Erfordernisse einer Anonymisierung/ Pseudonymisierung damit faktisch ausgehebelt. Dies lehnen wir ab. Zum Schutz der betroffenen Personen muss unseres Erachtens immer die Anonymisierung oder Pseudonymisierung geprüft und allenfalls aus Grunden der Unverhältnismäßigkeit davon abgesehen werden Alternative 1 sollte folglich gestrichen werden

Wir empfehlen außerdem ausdrücklich zu regeln, dass die Datensicherheit entsprechend § 78 PolG gewahrleistet werden muss, beispielsweise wie folgt.

„Die übermittelten Daten sind durch organisatorische und technische Maßnahmen entsprechend § 78 gegen unbefugte Kenntnisnahme zu schutzen "

Darüber hinaus empfehlen wir die Einfügung eines weiteren Absatzes mit folgendem Inhalt.

„Der Testungs- und Freigabeprozess eines KI-gestützten IT-Produkts wird in einer Verwaltungsvorschrift näher geregelt, die insbesondere die Schnittmengen zur KI-VO abbildet, die Nutzung von Reallaboren und eine Beteiligung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit vorsieht".

Die Voraussetzungen des Datenschutzrechts und der KI-Verordnung weisen Schnittmengen auf, die in systematischen Prozessen abgebildet werden sollten, für deren Erstellung auch rechtliche Expertise auf beiden Gebieten benötigt wird. Deswegen bietet sich die Vorstrukturierung des Testungs- und Freigabeprozesses in einer Verwaltungsvorschrift an. Die frühzeitige Einbindung des Landesbeauftragten ermöglicht eine fruhzeitige Beratung. Beides ist im Ubrigen - teilweise verpflichtend – in der KI-VO vorgesehen, s. Art. 57 Abs 10 KI-VO (Einbeziehung der Datenschutzaufsichtsbehörden) und Art. 59, 60 KI-VO (Nutzung von Reallaboren).

D. Zu § 74 Abs. 2 Nr. 1 PolG-E

Hier gilt das oben in Bezug auf die nicht hinreichende Bestimmtheit des Tatbestandsmerkmals „gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden" Gesagte: Unklar ist, was mit „weitere Maßnahmen" gemeint ist.

E. Zu § 86 Abs. 1 Nr. 1 PolG-E

Hier gilt das oben bereits Geschilderte: „weitere Maßnahmen" ist nicht hinreichend bestimmt

F. Zu § 98 Absatz 1 Nummer 14 PolG-E

Wir sind der Auffassung, dass nicht nur der Landesbeauftragte – dessen Aufgaben- und Personaldichte wir bereits in unserer letzten Stellungnahme dargelegt haben – Kontrollpflichten auferlegt werden sollten, sondern auch den verantwortlichen Stellen selbst. Es ist im Interesse der Polizei, selbst Erfahrungswerte zu sammeln, auszuwerten und Missbrauche durch Stichproben aufzuklären und zu ahnden. Selbstkontrolle stärkt das Vertrauen der Bevölkerung und sollte für eine mit machtigen Überwachungsmethoden ausgestattete Behörde als Kehrseite zu den eigenen Befugnissen zur Pflicht gehören.

Dazu begrüßen wir, dass in § 47a Abs. 4 Nr. 3 PolG-E das Konzept zur Zugriffskontrolle auch verdachtsunabhängige Stichprobenkontrollen der Zugriffe vorsieht. Wir regen darüber hinaus an, die absolute Anzahl an Zugriffen sowie die Anzahl an relevanten Erkenntnissen zu erfassen, damit die Häufigkeit der Nutzung und die Haufigkeit relevanter Ergebnisse evaluiert werden konnen

G. Zu § 4 DVO-PolG BW

Wie oben bereits dargelegt erlaubt die Verordnung nun voraussetzungslos die Delegation an den Polizeiführer vom Dienst. Dies wird der Erheblichkeit des Eingriffs unseres Erachtens nicht gerecht, vgl. oben.

Zusammenfassend empfehlen wir demnach insbesondere:

1. Die Anforderungen an die Erforderlichkeit zur Erfüllung der Eingriffsschwellen der automatisierten Datenanalyse sollten in der Gesetzesbegrundung dargelegt werden; denn klar sollte sein, dass die automatisierte Datenanalyse ein Instrument ist, dass nur dann zum Einsatz kommt, wenn es um erhebliche Gefahren geht und andere Mittel nicht zur Verfugung stehen.

2 Der Gesetzgeber hat darüber zu entscheiden, welche Informationen in eine Datenanalyse einbezogen werden dürfen. Art und Umgang der automatisiert analysierten Daten müssen daher durch den Gesetzgeber selbst konkretisiert werden.

3 Der Gesetzgeber sollte insbesondere entscheiden, wer „Unbeteiligter" im Sinne des Gesetzes sein soll.

4. Der Gesetzgeber sollte Daten offensichtlich Unbeteiligter nicht nur bezüglich der Vorgangsdaten fur die Datenanalyse sperren. Spätestens mit Ablauf der Übergangsfrist fur die Kennzeichnungspflicht aus § 72 PolG sollten die demzufolge verpflichtenden Informationen zum Schutze betroffener Personen genutzt werden.

5. Die Erlaubnis zum Einsatz Künstlicher Intelligenz bei der Datenanalyse muss mindestens durch eine Zweck-/ Zielsetzung durch den Gesetzgeber begrenzt werden Darüber hinaus sollte die Gesetzesbegründung die Risiken des Einsatzes kunstlicher Intelligenz vor dem konkreten Hintergrund der großen Datenmengen und polizeilichen Überwachungsbefugnissen adressieren.

6. Zur Abmilderung der Eingriffsintensitat und Ermoglichung einer Uberprufung einer automatisierten Datenanalyse sollte durch den Gesetzgeber klargestellt werden, was mit der tatbestandlichen Voraussetzung einer Benachrichtigungspflicht bei „weitere[n] Maßnahmen" gegen eine betroffene Person gemeint ist

7 Die Delegationsmoglichkeit der Anordnungsbefugnis an den Polizeifuhrer vom Dienst sollte durch den Gesetzgeber mit Voraussetzungen versehen werden.

8. Die Erlaubnis zur Vertestung von KI-gestützten IT-Produkten sollte rechtssicher mit der KI-VO verschrankt, insbesondere begriffliche Unklarheiten vermieden werden. Wir empfehlen eine ausdrückliche Regelung des Prufungs- und Freigabeprozesses durch eine Verwaltungsvorschrift. Anonymisierte/ pseudonymisierte Daten sollten klar vorzugswurdig bleiben.

Mit freundlichen Grußen
gez. [redacted]