

Antrag

des Abg. Sascha Binder u. a. SPD

und

Stellungnahme

**des Ministeriums des Inneren, für Digitalisierung
und Kommunen**

Verwendung der Palantir-Software in der Landesverwaltung Baden-Württemberg

Antrag

Der Landtag wolle beschließen,
die Landesregierung zu ersuchen
zu berichten,

1. wer zu welchem Zeitpunkt welche Verhandlungen mit der Firma Palantir geführt hat;
2. ob und inwieweit vor Vertragsunterzeichnung Kontakt zu anderen Bundesländern aufgenommen wurde, die die Palantir-Software bereits einsetzen oder vergleichbare Verträge geschlossen haben, um deren Erfahrungen und Informationen einzuholen unter besonderer Darstellung, welche Unterschiede es zu Vertragswerken anderer Bundesländer gibt;
3. wie die Landesregierung verhindern möchte, dass deutsche Zeugendaten an amerikanische Geheimdienste weitergegeben werden, wozu nach amerikanischem Recht eine Verpflichtung besteht;
4. welchen konkreten Inhalt der abgeschlossene Vertrag hat, insbesondere unter Darlegung, zu welchen Stichtagen jeweils Zahlungen in welcher Höhe fällig werden und welche Leistungen im Preis enthalten sind, insbesondere mit Blick auf Softwareupdates, Serviceleistungen und Schulungen;
5. in welcher Höhe weitere Kosten entstehen werden, insbesondere etwa für nicht vom Vertrag umfasste Dienstleistungen, Schulungen und Serverkapazitäten;
6. auf welche konkreten Datenbestände durch Palantir zugegriffen werden kann, insbesondere unter Bezug auf Daten von Nachrichtendiensten, die Staatsschutzdatei, INPOL, POLAS, ZEVIS und EMA;
7. wie der Umgang mit sensiblen Daten geregelt ist, insbesondere welche datenschutzrechtlichen, organisatorischen und technischen Maßnahmen zur Anwendung kommen, unter Darstellung inwieweit der Landesbeauftragte für den Datenschutz und die Informationsfreiheit einbezogen wurde bzw. ist;

Eingegangen: 11.8.2025 / Ausgegeben: 8.9.2025

1

8. ob es notwendig ist, dass Mitarbeitende von Palantir vor Ort, etwa beim Landeskriminalamt oder anderen Behörden, tätig werden, insbesondere bei der Verarbeitung personenbezogener Daten, und wenn ja, welche konkreten Tätigkeiten mit welchen Berechtigungen und Zugriffsmöglichkeiten auf personenbezogene Daten diese übernehmen;
9. wie Mitarbeitende von Palantir kontrolliert und beaufsichtigt werden, insbesondere hinsichtlich ihres Datenzugriffs;
10. ob Protokollierungs-Dateien erstellt werden, unter Darstellung, ob daraus ersichtlich ist, welche Daten von welchem Nutzer auf welche Weise und mit welchem Ergebnis ausgewertet wurden;
11. welche Vorgaben es für die weitere Verwendung der durch Palantir analysierten oder aufbereiteten Daten in der polizeilichen Arbeit gibt, insbesondere ob hierfür spezielle Akten oder Dokumentationsformen geschaffen werden;
12. ob und wenn ja in welchem Umfang insbesondere in Strafverfahren Akteneinsichtsrechte in Bezug auf durch Palantir generierte oder beeinflusste Informationen bestehen;
13. welche Einschränkungen der Nutzung der Innenminister in der Landespresskonferenz am 29. Juli 2025 konkret meinte, insbesondere mit Blick auf die Nutzung „getrennt vom öffentlichen Netz“ und die Nutzung von KI-Funktionalitäten sowie inwieweit bezahlte Funktionen der Software nach Vereinbarungen der Koalition nicht genutzt werden sollen;
14. zu welchem Zeitpunkt insbesondere mit Blick auf die notwendigen Änderungen im Polizeigesetz sowie die Implementierung von Palantir die Landesregierung von einer tatsächlichen Nutzbarkeit ausgeht;
15. welche Software Frankreich und Interpol nach ihrer Kenntnis aktuell nutzen unter Darstellung, inwiefern der Landesregierung bekannt ist, ob sie Palantir bereits genutzt haben.

8.8.2025

Binder, Ranger, Hoffmann, Dr. Weirauch, Weber SPD

Begründung

Der Einsatz von Softwarelösungen der Firma Palantir in sicherheitsrelevanten Bereichen der Landesverwaltung wirft zahlreiche rechtliche, technische und finanzielle Fragen auf. Eine transparente Darstellung der Vertragsinhalte, der Zugriffsbefugnisse sowie der organisatorischen und datenschutzrechtlichen Rahmenbedingungen ist unerlässlich, um eine informierte parlamentarische Bewertung und Kontrolle zu ermöglichen.

Stellungnahme

Mit Schreiben vom 2. September 2025 Nr. IM3-0141.5-651/73/2 nimmt das Ministerium des Inneren, für Digitalisierung und Kommunen zu dem Antrag wie folgt Stellung:

*Der Landtag wolle beschließen,
die Landesregierung zu ersuchen
zu berichten,*

1. wer zu welchem Zeitpunkt welche Verhandlungen mit der Firma Palantir geführt hat;

Zu 1.:

Im Zeitraum von November 2024 bis März 2025 führte das Präsidium Technik, Logistik, Service der Polizei (PTLS Pol), in enger Zusammenarbeit mit dem Landeskriminalamt (LKA), eine Reihe von vorvertraglichen Prüfungen und Vertragsverhandlungen durch. Die Verhandlungen erfolgten in Umsetzung des Beschlusses der Landesregierung, eine Verfahrenübergreifende Recherche- und Analyseplattform (VeRA) für die Polizei Baden-Württemberg zu implementieren, wie es im Maßnahmenpaket „Sicherheit stärken, Migration ordnen, Radikalisierung vorbeugen“ vom 23. September 2024 festgelegt wurde. Das PTLS Pol wurde mit gesondertem Schreiben des Ministeriums des Inneren, für Digitalisierung und Kommunen – Landespolizeipräsidium (IM-LPP) vom 18. Oktober 2024 beauftragt, den Rahmenvertrag, den der Freistaat Bayern im März 2022 mit dem Unternehmen Palantir Technologies GmbH (Palantir) verhandelt hatte, als Grundlage für die Umsetzung zu nehmen, da aus diesem alle Bundesländer abrufberechtigt sind. Eine Ausschreibung durch Baden-Württemberg war somit nicht erforderlich.

Am 29. Januar 2025 erfolgte der maßgebliche Abstimmungstermin im LKA. An diesem Termin nahmen Vertreter des PTLS Pol, des LKA sowie der Firma Palantir teil. Durch den Abruf aus dem bayerischen Rahmenvertrag waren keine individuellen Verhandlungen für die Polizei Baden-Württemberg erforderlich. Die Vertragsverhandlungen konzentrierten sich daher ausschließlich auf die Ausarbeitung der Ergänzenden Vertragsbedingungen für die Beschaffung eines IT-Systems (EVB-IT Systemvertrag¹) sowie der Auftragsdatenverarbeitung für Baden-Württemberg. Die grundsätzlichen Rahmenparameter des Vertrags, wie beispielsweise Laufzeiten, Kündigungsmöglichkeiten oder Konditionen, waren durch die Rahmenvereinbarung bereits verbindlich festgelegt.

2. ob und inwieweit vor Vertragsunterzeichnung Kontakt zu anderen Bundesländern aufgenommen wurde, die die Palantir-Software bereits einsetzen oder vergleichbare Verträge geschlossen haben, um deren Erfahrungen und Informationen einzuholen unter besonderer Darstellung, welche Unterschiede es zu Vertragswerken anderer Bundesländer gibt;

Zu 2.:

Die Vertragsunterzeichnung zwischen dem Land Baden-Württemberg, vertreten durch das PTLS Pol, und Palantir erfolgte am 20. März 2025 durch die Dienststellenleitung des PTLS Pol. Dies vor dem Hintergrund, dass beim PTLS Pol die Vergabestelle der Polizei Baden-Württemberg angesiedelt ist. Zudem ist das PTLS Pol eine zentrale Dienstleistungs- und Serviceeinheit der Polizei Baden-Württemberg und u. a. für den landesweiten IT-Betrieb der Polizei verantwortlich.

Vor Vertragsunterzeichnung wurde Kontakt zu den Ländern Bayern, Hessen und Nordrhein-Westfalen aufgenommen. Die Vertragswerke der genannten Bundesländer sind hier nicht bekannt, insofern liegen auch keine Erkenntnisse zu Übereinstimmungen oder Unterschieden vor.

¹ Ein EVB-IT Systemvertrag ist ein standardisiertes Vertragsmuster für die öffentliche Hand in Deutschland, das zur Beschaffung und Integration von IT-Systemen, bestehend aus mehreren Komponenten und/oder verschiedenen Leistungen, verwendet wird.

Bayern

Aus dem vom Freistaat Bayern mit Palantir geschlossenen Mantel-Rahmenvertrag für die Beschaffung einer VeRA vom 4. März 2022 ergibt sich für die Länder die Möglichkeit, ohne nochmaliges Vergabeverfahren, einen EVB-IT Systemvertrag mit Palantir abzuschließen und vertragsgegenständliche Leistungen abzurufen. Hierzu wurden im Vergabeverfahren zum Mantel-Rahmenvertrag mit Palantir feste Lizenzgebühren für die beteiligten Länder ausgehandelt. Das Preisblatt sieht für Lizenzabrufe der Länder, die nach den ersten drei Jahren nach Zuschlagserteilung (Stichtag war der 21. März 2025) erfolgen, eine signifikante Preiserhöhung vor.

Am 12. November 2024 fand eine Besprechung zwischen Vertretern des PTLS Pol und des Bayerischen Landeskriminalamts statt. Bei diesem Termin stand der Erfahrungsaustausch im Vordergrund. Die Einführung von Palantir in Bayern hat eine Vielzahl von Erfahrungen und Erkenntnissen hervorgebracht. Des Weiteren konnten gewinnbringende Erfahrungen zum Betrieb der umfangreichen und technisch anspruchsvollen Plattform gewonnen werden, die in die eigenen Planungen miteinbezogen wurden.

Hessen

Am 18. und 19. November 2024 besuchte eine Delegation des PTLS Pol den Innovation Hub 110 der Hessischen Polizei in Frankfurt am Main. Ziel des Termins war, Gespräche zu strategischen und operativen Themenfeldern zu führen, insbesondere im Hinblick auf die hessische Polizei-Plattform „hessenDATA“. Im Rahmen des Austauschs wurden die Möglichkeiten einer perspektivischen Zusammenarbeit zwischen den beteiligten Partnern zur Umsetzung der VeRA für die Polizei Baden-Württemberg sondiert. Der Termin wurde ebenfalls genutzt, um Erfahrungswerte und Eindrücke für „hessenDATA“ zu erhalten und wiederum für die eigene Projektarbeit zu nutzen.

Nordrhein-Westfalen

Auf Fachebene wurden im Vorfeld der Vertragsunterzeichnung Informationen zur Zusammenarbeit der Polizei Nordrhein-Westfalen mit Palantir erhoben und ebenso entsprechende Erfahrungswerte sowie das Interesse zur Teilnahme an einer Betriebskooperation erfragt. Eine vertiefende Zusammenarbeit kam nicht zustande.

3. wie die Landesregierung verhindern möchte, dass deutsche Zeugendaten an amerikanische Geheimdienste weitergegeben werden, wozu nach amerikanischem Recht eine Verpflichtung besteht;

Zu 3.:

Um die IT-Sicherheit und den Datenschutz zu gewährleisten, werden in der Umsetzung der VeRA perspektivisch unterschiedliche Maßnahmen ergriffen. Die Plattform VeRA wird ausschließlich auf einer polizeieigenen IT-Infrastruktur betrieben (On-Premise). Dies bedeutet, dass alle Daten im besonders gesicherten polizeilichen Netz bleiben und nicht in Drittstaaten oder in eine externe Cloud-Infrastruktur übertragen werden können. Die Datenhoheit sowie die physische und logische Kontrolle über Server und Netzwerkinfrastruktur liegt ausschließlich bei der Polizei Baden-Württemberg. Damit hat Palantir als Softwareanbieter keinen eigenständigen Zugriff auf die Plattform. Diese Mechanismen ermöglichen eine präzise Steuerung aller Verarbeitungen und Zugriffe. Die technische Architektur der Plattform ist von Grund auf darauf ausgelegt, jede unbefugte Verarbeitung zu verhindern („Zero Trust“). Im Ergebnis werden unterschiedliche Sicherheits- und Datenschutzarchitekturen angewendet, welche durch eine Kombination aus technischen, vertraglichen und organisatorischen Maßnahmen sicherstellen, dass ein Datenabfluss aus dem System verhindert wird. Selbst bei einem nach allen Rechtsordnungen rechtmäßigen Zugriffsgesuch würden bei einem On-Premise-Betrieb der VeRA technische und tatsächliche Zugriffsmöglichkeiten nicht gegeben sein. Die Datenverarbeitung verbleibt vollständig unter der Kontrolle des Landes Baden-Württemberg.

Alle Mitarbeiterinnen und Mitarbeiter von Palantir werden – wie alle externen Dienstleister – gemäß den gültigen Regularien sicherheitsüberprüft. Die Polizei Baden-Württemberg orientiert sich hierzu überwiegend an den Erfahrungen aus

Hessen, die im Rahmen der Einführung von „hessenDATA“ gesammelt wurden. Der Betrieb von „hessenDATA“ erfolgt innerhalb des abgesicherten Polizeinetzes und die Datenhoheit sowie die vollständige Kontrolle über die zu verarbeitenden Daten und die Analyseplattform selbst liegen ausschließlich bei der hessischen Polizei. Grundsätzlich werden die VeRA sowie die dort verarbeiteten polizeilichen Daten auf polizeieigenen Servern im Rechenzentrum der HZD verortet sein. Mitarbeiter von Palantir haben weder unbeaufsichtigte Zutrittsmöglichkeiten in dieses Rechenzentrum, noch haben sie technisch die Möglichkeit, Daten aus den polizeilichen Systemen auszuleiten oder einzubringen. Die Datenhoheit und die Kontrolle über das System liegen vollständig bei der Polizei Baden-Württemberg. Des Weiteren haben die sicherheitsüberprüften Mitarbeitenden von Palantir ausschließlich zur technischen Weiterentwicklung und Fehlerbehebung Zugriff auf die zu dieser Aufgabe benötigten technischen Bereiche des Systems.

4. welchen konkreten Inhalt der abgeschlossene Vertrag hat, insbesondere unter Darlegung, zu welchen Stichtagen jeweils Zahlungen in welcher Höhe fällig werden und welche Leistungen im Preis enthalten sind, insbesondere mit Blick auf Softwareupdates, Serviceleistungen und Schulungen;

Zu 4.:

Die genauen Inhalte des Vertrags des PTL Pol mit Palantir unterliegen der Geheimhaltung. Gleiches gilt für die Verträge der Bundesländer Hessen und Bayern mit Palantir.

Aus der sorgfältigen Abwägung der verfassungsrechtlich garantierten Informationsrechte der Abgeordneten mit dem Staatswohl und der Grundrechte Dritter folgt, dass dem Staatswohl und den Grundrechten Dritter Vorrang einzuräumen ist.

Der Aufbau und Betrieb der VeRA sind für die Polizei Baden-Württemberg besonders sensible Verfahren, da einerseits technisch höchst komplexe Systeme zum Einsatz kommen, personenbezogene Daten mit diesem Verfahren verarbeitet werden (können) und zusätzlich Ermittlungs- und Analyseverfahren, Strukturen und Taktiken abgebildet werden. Die Funktionalitäten der VeRA kommen bei kriminalpolizeilichen Maßnahmen zum Einsatz, um als „Werkzeug“ bei hochkomplexen Sachverhalten eine technische Hilfestellung zu bieten. Die Veröffentlichung von Vertragsinhalten würde – neben tiefgehenden Einblicken in das Geschäftsmodell, die Rahmenbedingungen und Konditionen – auch Informationen zu den technischen Spezifikationen der Plattform wie Integrationsmöglichkeiten oder spezifischen Analysefunktionalitäten liefern. Die Vertragsunterlagen beinhalten, insbesondere in der Leistungsbeschreibung, Informationen zu Anwendungsfällen, welche die Polizei Baden-Württemberg mit der Software bearbeiten möchte. In diesem Kontext werden Funktionen der VeRA erklärt oder dargestellt, welche kriminellen Personen wertvolle Informationen über die aktuellen und zukünftigen Ermittlungs- und Auswertemethoden der Polizei Baden-Württemberg, aber auch anderer Sicherheitsbehörden bundesweit, liefern würden. Dadurch wären Rückschlüsse auf das polizeiliche Handeln möglich und diese Personen könnten Straftaten besser planen und die Ermittlungsarbeit der Sicherheitsbehörden dadurch massiv erschweren oder im schlimmsten Fall gar umgehen. Die Herausgabe von konkreten Vertragsinhalten gefährdet somit die Wirksamkeit sicherheitsbehördlicher Maßnahmen und damit die verfassungsrechtliche Gewährleistung einer funktionsfähigen Gefahrenabwehr und Strafverfolgung. Dieses Risiko kann unter keinen Umständen hingenommen werden.

Würde bekannt, dass das Land Baden-Württemberg entgegen vertraglicher Vereinbarungen Informationen bekannt gibt, würde dies Nachteile für zukünftige Vertragsabschlüsse mit anderen Wirtschaftsunternehmen nach sich ziehen. Für die Funktionsfähigkeit des Staats ist es elementar, vertrauensvoll mit Unternehmen der Privatwirtschaft zusammenzuarbeiten.

Die Palantir Technologies GmbH als Vertragspartnerin ist ein inländisches Unternehmen und damit grundrechtsberechtigt. Bei der sorgfältigen Abwägung des Informationsinteresses des Parlaments mit den Grundrechten Dritter – z. B. dem Schutz des Eigentums der Palantir Technologies GmbH – wurde geprüft, ob andere Formen der Informationsübermittlung möglich sind. Eine Herausgabe der

Vertragsunterlagen mit Schwärzungen ist nicht praktikabel. Die schützenswerten Informationen durchziehen sämtliche Vertragsdokumente so umfassend, dass nach den erforderlichen Schwärzungen kein sinnvoller Informationsgehalt mehr verbleiben würde. Zudem können bereits aus fragmentarischen Informationen sachkundige Dritte weitreichende Rückschlüsse auf Geschäftsgeheimnisse und die Systemarchitektur ziehen. Auch ist die Preisgestaltung untrennbar mit den Leistungsbeschreibungen verknüpft. Technische Spezifikationen finden sich in nahezu allen Vertragsabschnitten. Selbst scheinbar harmlose Angaben wie Nutzeranzahlen oder Datenvolumina ermöglichen in ihrer Gesamtschau Rückschlüsse auf die Systemarchitektur und Preisbildung. Ein Bekanntwerden dieser Informationen würde zudem mit Wettbewerbsnachteilen und irreversiblen wirtschaftlichen Schäden (z. B. Verlust von Alleinstellungsmerkmalen) für die Palantir Technologies GmbH einhergehen und einen Haftungsanspruch des Unternehmens gegenüber dem Herausgeber der Informationen bewirken.

Die Landesregierung hat in die Abwägung zudem einbezogen, ob eine eingestufte Form der Informationsübermittlung möglich ist, die das Informationsinteresse des Landtags unter Wahrung berechtigter Geheimhaltungsinteressen der Landesregierung befriedigt. Die erbetenen Informationen berühren jedoch derart die dargestellten schutzbedürftigen Belange, dass auch ein geringfügiges Risiko des Bekanntwerdens im Falle einer eingestuften Stellungnahme nicht hingenommen werden kann. Über den konkreten Inhalt des Vertrags ist daher nicht nur aus verfassungsrechtlichen Gründen Stillschweigen zu wahren. Hierzu besteht auch eine vertragliche Verpflichtung für das Land Baden-Württemberg.

Jedoch kann Folgendes mitgeteilt werden:

Der Vertrag umfasst die Nutzung des Softwareprodukts „Gotham“ mit einer eingeschränkten Version des Softwareprodukts „Foundry“ und hat ein Gesamtvolumen von rund 25 Millionen Euro über eine Laufzeit von fünf Jahren. In dieser Grundkonfiguration der VeRA sind die Recherche- und Analysevorgänge auf die angebundenen Quellsysteme beschränkt. Mit Quellsystemen sind Fachverfahren gemeint, wie etwa Daten aus polizeilichen Auskunftssystemen oder dem Vorgangsbearbeitungssystem der Polizei Baden-Württemberg. Diese sollen in der VeRA automatisiert zusammengeführt werden können.

Palantir überlässt die Software nicht nur zur Nutzung, sondern übernimmt beispielsweise auch noch Installation und Anpassung der Soft- und Hardware auf die Bedürfnisse der Polizei Baden-Württemberg. Daneben sind Wartungstätigkeiten (z. B. Installation von Updates, Störungsbeseitigung) und in begrenztem Umfang Schulungsleistungen vertraglich vereinbart. Es lässt sich daher nicht ausschließen, dass ein Tätigwerden von Mitarbeitenden von Palantir vor Ort in polizeilichen Liegenschaften (PTLS Pol, LKA) notwendig werden kann. Alle Mitarbeitende von Palantir werden – wie alle externen Dienstleister – gemäß den gültigen Regularien sicherheitsüberprüft. Die Polizei Baden-Württemberg orientiert sich hierzu überwiegend an den Erfahrungen aus Hessen, die im Rahmen der Einführung von „hessenDATA“ gesammelt wurden (detaillierte hierzu Antwort zu Ziffer 8 und 9). Bei den zugrundeliegenden Softwareprodukten von Palantir handelt es sich um hochgradig komplexe Systeme, die ohne diese anlassbezogene Unterstützung durch Palantir nicht betrieben werden können.

Der Vertrag sieht vor, dass die Kosten für die Softwarelizenz erstmals mit der Systemeinführung (Bereitstellung von Soft-/Hardware durch Palantir) in Rechnung gestellt werden. Grundsätzlich erfolgt die Zahlung der Lizenzkosten quartalsweise im Voraus. Unabhängig vom Zeitpunkt der tatsächlichen Inbetriebnahme endet der Vertrag nach fünf Jahren. Optional besteht die Möglichkeit, den Vertrag nach der Grundlaufzeit bis zu vier Mal um jeweils ein Jahr zu verlängern. Mit Beschluss vom 29. Juli 2025 wurde vom Ministerrat festgelegt, dass von dieser Option kein Gebrauch gemacht wird. Eine Verpflichtung zur Nutzung der Software besteht nicht. Vertraglich besteht ein Nutzungsrecht, vergleichbar mit einer „Flatrate“. Die Systemeinführung soll nach derzeitigen Planungen noch im Jahr 2025 erfolgen.

5. in welcher Höhe weitere Kosten entstehen werden, insbesondere etwa für nicht vom Vertrag umfasste Dienstleistungen, Schulungen und Serverkapazitäten;

Zu 5.:

Neben den Kosten für Software und Hardware von Palantir fallen noch weitere Kosten gegenüber anderen Auftragnehmern an. Hierbei handelt es sich um deutsche bzw. europäische Unternehmen mit welchen die Polizei Baden-Württemberg in verschiedensten Bereichen, teilweise seit vielen Jahren, gut zusammenarbeitet sowie um die Hessische Zentrale für Datenverarbeitung (HZD). Diese Kosten umfassen verschiedene Komponenten, die für die Umsetzung und den Betrieb des Vorhabens VeRA notwendig sind. Zunächst ist die VeRA-Hardware zu nennen, die mit einer einmaligen Investition verbunden ist. Darüber hinaus fallen laufende Kosten für die Anbindung des Rechenzentrums STACKIT in Neckarsulm mit dem Ziel-Rechenzentrum der HZD in Wiesbaden an. Weitere Kosten entstehen bei der HZD für den Betrieb der Hard- und Software. Darüber hinaus plant das PTLs Pol mit Kosten für externe Dienstleister für die Systemintegration. In der Gesamtschau wird derzeit mit weiteren Kosten in Höhe von etwa 2 Mio. Euro gerechnet.

6. auf welche konkreten Datenbestände durch Palantir zugegriffen werden kann, insbesondere unter Bezug auf Daten von Nachrichtendiensten, die Staatsschutzdatei, INPOL, POLAS, ZEVIS und EMA;

Zu 6.:

Die Software von Palantir soll personenbezogene Daten, die die Polizei Baden-Württemberg zuvor rechtmäßig erhoben und gespeichert hat, in einer VeRA im Rahmen der automatisierten Datenanalyse zusammenführen können. Das Bundesverfassungsgericht hat in seinem Urteil vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20) die Nutzung einer automatisierten Datenanalyse dem Grunde nach für zulässig erklärt und die Voraussetzungen für eine verfassungskonform ausgestaltende Rechtsgrundlage genannt. An dieser höchstrichterlichen Rechtsprechung orientiert sich der aktuelle Gesetzentwurf zur Änderung des Polizeigesetzes Baden-Württemberg (PolG), der den im Landtag von Baden-Württemberg vertretenen Fraktionen mit Schreiben vom 30. Juli 2025 zugeht. Der Gesetzentwurf enthält in § 47a PolG-E eine entsprechende Rechtsgrundlage für die automatisierte Datenanalyse. Die folgenden Ausführungen beziehen sich daher auf die zugehörige Begründung zu § 47a PolG-E im aktuellen Gesetzentwurf.

In § 47a PolG-E Absatz 3 soll abschließend bestimmt werden, welche Datenbestände und Daten auf der Analyseplattform zusammengeführt werden dürfen. Dabei soll zwischen Datenbeständen unterschieden werden, die auf der Plattform laufend zusammengeführt werden, und solchen Daten, die einzelfallbezogen in die Analyse einbezogen werden. Hiermit wird sowohl die Art der zu verarbeitenden Daten als auch deren Umfang hinreichend bestimmt und zudem verhältnismäßig abgestuft, um das Eingriffsgewicht der automatisierten Datenanalyse nach den Vorgaben des Bundesverfassungsgerichts zu mindern. Zum Zweck der automatisierten Datenanalyse sollen eigene Vorgangsdaten, Falldaten, Daten aus polizeilichen Auskunftssystemen und Daten aus dem polizeilichen Informationsaustausch zusammengeführt werden können. Die positive Benennung der zum Zweck der automatisierten Datenanalyse nutzbaren Quellen hat den Charakter einer abschließenden Regelung und soll damit gleichzeitig eine Begrenzung der Datenmenge enthalten. Die zusätzliche Einschränkung auf eigene Daten soll klarstellen, dass es sich um Daten handelt, welche die Polizei Baden-Württemberg als verantwortliche Stelle in den eigenen polizeilichen Dateisystemen gespeichert hat. Nachrichtendienstliche Quellsysteme dürfen, auch aufgrund des Trennungsgebots, nicht einbezogen werden.

Vorgangsdaten sind sämtliche Unterlagen, die im Zusammenhang mit einer polizeilichen Tätigkeit bei einem bestimmten Einsatzanlass zu Personen und Sachen im polizeilichen Vorgangsbearbeitungssystem erfasst werden. 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, soll in § 47a PolG-E Absatz 6

Satz 3 geregelt werden, dass deren Vorgangsdaten nicht in die automatisierte Datenanalyse einbezogen werden dürfen. Hierdurch wird die Eingriffsintensität reduziert. Ausgangspunkt ist die Differenzierung nach einerseits verurteilten, beschuldigten, verdächtigen und sonstigen Anlasspersonen sowie deren Kontaktpersonen und andererseits unbeteiligten Personen. Bei Daten, die von der Kennzeichnungspflicht nach § 72 PolG umfasst sind – hierzu gehören grundsätzlich auch Vorgangsdaten, wird im Umfang des gesetzlich vorgegebenen Umsetzungsstandes durch die vorzunehmende Kategorisierung gewährleistet, dass Daten unbeteiligter Personen im polizeilichen Sinne nicht einbezogen werden.

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 enthalten 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.

§ 47a PolG-E Absatz 3 Satz 2 soll 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 regeln.

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 soll im Einzelfall dann möglich sein, wenn mindestens tatsächliche Anhaltspunkte dafür vorliegen, dass das einzubindende Asservat in Verbindung zum konkreten Suchanlass steht.

Daten anderer Polizeien sind nicht von § 47a PolG-E Absatz 3 Satz 1 umfasst. In gezielten Einzelabfragen erhobene Daten, die andere Polizeien als verantwortliche Stelle in ihren polizeilichen Dateisystemen gespeichert haben, sollen über Satz 2, soweit erforderlich, ergänzend in die Analyse einbezogen werden können.

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 sollen, 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 infrage steht. Hat diese Person eine Waffenerlaubnis, kann darin ein gefahrerhöhendes Indiz gesehen werden.

§ 47a PolG-E Absatz 3 Satz 2 soll zudem eine ergänzende Einbeziehung von gesondert gespeicherten Datensätzen aus Internetquellen erlauben. Da gemäß § 47a PolG-E Absatz 2 Satz 6 eine direkte Anbindung der Analyseplattform an Internetdienste unzulässig sein soll, dürfen diese Daten nicht automatisiert einbezogen werden. Vielmehr sollen sie für jeden Analysevorgang händisch hinzugezogen werden müssen. Es handelt sich bei den einbezogenen Datensätzen regelmäßig um die aufbereiteten und bereits gefilterten Ergebnisse polizeilicher Recherchen.

Voraussetzung soll sein, dass die Einbeziehung dieser Daten zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist.

Nach § 47a PolG-E Absatz 3 Satz 3 sollen Verkehrsdaten aus Funkzellenabfragen sowie Telekommunikationsdaten nicht in die automatisierte Datenanalyse einbezogen werden dürfen, wenn die Maßnahme gemäß § 47a PolG-E 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 soll sowohl dem Schutz unbeteiligter Personen als auch der Wahrung der Verhältnismäßigkeit dienen. Darüber hinaus sollen auch Telekommunikationsdaten nicht in die automatisierte Datenanalyse gemäß § 47a PolG-E Absatz 1 Nummer 3 einbezogen werden dürfen, 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.

Zur Verringerung der Eingriffsintensität der automatisierten Datenanalyse soll beitragen, dass nach § 47a PolG-E Absatz 3 Satz 6 personenbezogene Daten, die aus den besonders schwerwiegenden Grundrechtseingriffen der Wohnraumüberwachung und der Online-Durchsuchung stammen, nicht einbezogen werden dürfen.

- 7. wie der Umgang mit sensiblen Daten geregelt ist, insbesondere welche datenschutzrechtlichen, organisatorischen und technischen Maßnahmen zur Anwendung kommen, unter Darstellung inwieweit der Landesbeauftragte für den Datenschutz und die Informationsfreiheit einbezogen wurde bzw. ist;*
- 10. ob Protokollierungs-Dateien erstellt werden, unter Darstellung, ob daraus ersichtlich ist, welche Daten von welchem Nutzer auf welche Weise und mit welchem Ergebnis ausgewertet wurden;*
- 11. welche Vorgaben es für die weitere Verwendung der durch Palantir analysierten oder aufbereiteten Daten in der polizeilichen Arbeit gibt, insbesondere ob hierfür spezielle Akten oder Dokumentationsformen geschaffen werden;*

Zu 7. sowie 10. und 11.:

Zu den Ziffern 7 sowie 10 und 11 wird aufgrund des Sachzusammenhangs gemeinsam Stellung genommen.

Die Anwendung einer Software zur automatisierten Datenanalyse soll gemäß den Regelungen im aktuellen Gesetzentwurf – den Vorgaben des Bundesverfassungsgerichts in seinem Urteil vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20) entsprechend – umfassenden Kontrollmechanismen unterliegen, um den Schutz sensibler Daten sicherzustellen. Dazu gehören unter anderem technisch-organisatorische Vorkehrungen über ein noch in Bearbeitung befindliches Rollen- und Rechtekonzept, in welchem festzulegen ist, wer innerhalb der Polizei Baden-Württemberg Zugriff auf welche Daten haben kann und mit welchen Rechten und Pflichten der Zugriff verbunden ist, sowie über ein noch in Bearbeitung befindliches Konzept zur Zugriffskontrolle, das auch verdachtsunabhängige Stichprobenkontrollen der Zugriffe vorsieht. Die Zugriffskontrolle wird durch die Protokollierung der einzelnen Arbeitsschritte gemäß § 74 PolG (Protokollierungspflicht bei verdeckten und eingriffsintensiven Maßnahmen) abgesichert. Auf diese Weise wird sichergestellt, dass nur berechnigte Personen eine automatisierte Datenanalyse vornehmen können. Die gesetzlich vorgeschriebene Protokollierung sichert die nachträgliche aufsichtliche Kontrolle. Darüber hinaus wird derzeit ein Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten erarbeitet, welches zu einer Begrenzung des Datenbestandes und damit zu einer Verringerung der Eingriffsintensität beiträgt.

Die vorgenannten Konzepte sind dabei in einer noch zu erlassenden Verwaltungsvorschrift festzuschreiben. Zudem sollen Maßnahmen der automatisierten Datenanalyse nur auf schriftliche und begründete Anordnung der Behördenleitung – bei Gefahr im Verzug auch durch besonders beauftragte Beamtinnen und Beamte

– erfolgen dürfen. Des Weiteren ist vorgesehen, dass der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI) vor der Einrichtung oder wesentlichen Änderung der Analyseplattform anzuhören ist. Zur Gewährleistung der Transparenz soll darüber hinaus die parlamentarische Kontrolle erweitert werden. Dies soll das Parlamentarische Kontrollgremium übernehmen.

Die weitere Verarbeitung der durch die Software zur automatisierten Datenanalyse aufbereiteten Daten richtet sich nach den Grundsätzen der Zweckbindung und Zweckänderung, was im Entwurf der Rechtsgrundlage verankert wurde.

Der LfDI wurde bereits bei der Erstellung des ersten Referentenentwurfes eingebunden. Im Rahmen des offiziellen Beteiligungsverfahrens zum ersten sowie zum zweiten Referentenentwurf wurde der LfDI ebenfalls beteiligt.

8. ob es notwendig ist, dass Mitarbeitende von Palantir vor Ort, etwa beim Landeskriminalamt oder anderen Behörden, tätig werden, insbesondere bei der Verarbeitung personenbezogener Daten, und wenn ja, welche konkreten Tätigkeiten mit welchen Berechtigungen und Zugriffsmöglichkeiten auf personenbezogene Daten diese übernehmen;

9. wie Mitarbeitende von Palantir kontrolliert und beaufsichtigt werden, insbesondere hinsichtlich ihres Datenzugriffs;

Zu 8. und 9.:

Zu den Ziffern 8 und 9 wird aufgrund des Sachzusammenhangs gemeinsam Stellung genommen.

Alle Mitarbeiterinnen und Mitarbeiter von Palantir werden – wie alle externen Dienstleister – gemäß den gültigen Regularien sicherheitsüberprüft. Die Polizei Baden-Württemberg orientiert sich hierzu überwiegend an den Erfahrungen aus Hessen, die im Rahmen der Einführung von „hessenDATA“ gesammelt wurden. Der Betrieb von „hessenDATA“ erfolgt innerhalb des abgesicherten Polizeinetzes und die Datenhoheit sowie die vollständige Kontrolle über die zu verarbeitenden Daten und die Analyseplattform selbst liegen ausschließlich bei der hessischen Polizei. Grundsätzlich werden die VeRA sowie die dort verarbeiteten polizeilichen Daten auf polizeieigenen Servern im Rechenzentrum der HZD verortet sein. Mitarbeiter von Palantir haben weder unbeaufsichtigte Zutrittsmöglichkeiten in dieses Rechenzentrum, noch haben sie technisch die Möglichkeit, Daten aus den polizeilichen Systemen auszuleiten oder einzubringen. Die Datenhoheit und die Kontrolle über das System liegen vollständig bei der Polizei Baden-Württemberg. Des Weiteren haben die sicherheitsüberprüften Mitarbeitenden von Palantir ausschließlich zur technischen Weiterentwicklung und Fehlerbehebung Zugriff auf die zu dieser Aufgabe benötigten technischen Bereiche des Systems.

Es lässt sich nicht ausschließen, dass ein Tätigwerden von einzelnen Mitarbeitern von Palantir vor Ort in polizeilichen Liegenschaften (PTLS Pol, LKA) notwendig werden kann. Die Einführung der VeRA in Baden-Württemberg wird nach derzeitigem Planungsstand in zwei Phasen erfolgen: Phase 1 (Projekt) und Phase 2 (Betrieb). Während der Phase 1 finden regelmäßige Abstimmungsgespräche zwischen Palantir und dem PTLs Pol statt, um gemeinsam alle notwendigen Rahmenbedingungen zur erfolgreichen Umsetzung des Vorhabens zu schaffen. In der Phase 2 werden anlassbezogene Termine vor Ort bei der HZD in Wiesbaden sowie vor Ort bei der Polizei Baden-Württemberg und/oder Remote regelmäßig notwendig werden, um spezifische Themenstellungen sowie neue oder geänderte Anforderungen und Fragestellungen klären zu können. Das Verfahren orientiert sich an einem gesonderten Rechte- und Rollenkonzept, welches in den Prozess implementiert wird und den Zugriff innerhalb der Software regelt. Darüber hinaus wird es eine gesonderte Protokollierungsfunktion geben, damit nachvollzogen werden kann, wer zu welchem Zeitpunkt auf welche Daten zugegriffen hat.

12. ob und wenn ja in welchem Umfang insbesondere in Strafverfahren Akteneinsichtsrechte in Bezug auf durch Palantir generierte oder beeinflusste Informationen bestehen;

Zu 12.:

Der Einsatz einer Software zur automatisierten Datenanalyse nach dem Polizeigesetz dient dem Zweck der Gefahrenabwehr. Bei Vorliegen der gesetzlichen Voraussetzungen können im Zuge der Gefahrenabwehr gewonnene Informationen auch in ein Strafverfahren eingeführt werden. Im Rahmen eines Strafverfahrens besteht gemäß § 147 StPO grundsätzlich ein Recht auf vollständige Einsicht in die Akten und Beweisstücke. Hiervon erfasst sind auch Daten, bei denen die automatisierte Datenanalyse die Recherche und Analyse unterstützt hat.

13. welche Einschränkungen der Nutzung der Innenminister in der Landespresseskonferenz am 29. Juli 2025 konkret meinte, insbesondere mit Blick auf die Nutzung „getrennt vom öffentlichen Netz“ und die Nutzung von KI-Funktionalitäten sowie inwieweit bezahlte Funktionen der Software nach Vereinbarungen der Koalition nicht genutzt werden sollen;

Zu 13.:

Das Konzept des Innenministeriums ist sowohl kurzfristig als auch langfristig auf den bestmöglichen Schutz der Menschen im Land ausgerichtet. Kurzfristig soll zeitnah die Software von Palantir eingesetzt werden – und zwar als Zwischenlösung für einen begrenzten Zeitraum. Für die Zeit danach hat Innenminister Thomas Strobl eine Kooperation mit qualifizierten Partnern auf den Weg gebracht, um eine souveräne europäische Software, eine Europa-VeRA, zu entwickeln. Diese soll den Sicherheitsbehörden die notwendigen technischen Fähigkeiten zur Recherche und Analyse großer Mengen polizeilicher Daten langfristig und unabhängig gewährleisten. Initiale Projektpartner sind zunächst die Airbus Defence and Space GmbH und die Digitalsparte der Schwarz Gruppe, Schwarz Digits. Weitere Unternehmen können folgen. Baden-württembergische Sicherheitsbehörden begleiten dieses Projekt eng mit Blick auf die spezifischen fachlichen Bedarfe an eine VeRA.

Bei der Landespresseskonferenz am 29. Juli 2025 wurde u. a. dargestellt, dass die Nutzung der Software von Palantir auf gesetzlicher Grundlage erfolgen wird sowie unter Einhaltung aller datenschutzrechtlichen Vorgaben. Die Nutzung des Systems erfolgt getrennt vom öffentlichen Netz, d. h. es gibt keine direkte Anbindung der Analyseplattform an Internetdienste oder Social-Media-Plattformen. Der Betrieb von VeRA findet im Polizeinetz (On-Premise), ausschließlich in gesicherten Rechenzentren in Deutschland unter Hoheit der Polizei statt und erfolgt unter eigenen technischen Rahmenbedingungen, die regelmäßig überprüft und weiterentwickelt werden. Dabei werden alle relevanten Aspekte, insbesondere im Zusammenhang mit der Informationssicherheit und Betriebsstabilität, fortlaufend berücksichtigt. Die Software von Palantir ist in den Punkten IT-Sicherheit und Datenschutz umfassend geprüft. Ein Zugriff durch ausländische Stellen ist ausgeschlossen. Von Anfang an war der LfDI bei der Erarbeitung der gesetzlichen Grundlage eingebunden. Eine Zusammenarbeit mit dem LfDI erfolgt auch bei der Einführung der Software.

Im Kontext Datensicherheit wurden weitgehende Sicherungsmaßnahmen für die Nutzung der VeRA durch die Polizei Baden-Württemberg getroffen: Im Vertrag mit Palantir sind Vereinbarungen zur IT-Sicherheit enthalten. Demnach dürfen die Software selbst und auch Updates unter anderem keine Funktionen zum unerwünschten Absetzen/Ausleiten von Daten, Funktionen zur unerwünschten Veränderung/Manipulation von Daten oder Funktionen zum unerwünschten Einleiten von Daten oder unerwünschte Funktionserweiterungen (sog. Backdoors) enthalten.

Das Fraunhofer Institut hat den Quellcode untersucht und keine Funktionalitäten festgestellt, die einen unzulässigen Datenabfluss oder einen unautorisierten Systemzugriff ermöglichen.

Zur Gewährleistung der Transparenz hinsichtlich des neuen Werkzeugs soll darüber hinaus die parlamentarische Kontrolle erweitert werden. Dies soll das Parlamentarische Kontrollgremium übernehmen und vier Mal im Jahr erfolgen. Gemäß

Kabinettsvorlage zur Freigabe der Anhörung des Entwurfs eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften vom 29. Juli 2025 wurde vom Ministerrat festgelegt, dass die Nutzung von KI-Produkten von Palantir ausdrücklich ausgeschlossen ist und mit Ablauf der fünfjährigen Vertragslaufzeit der bestehende Vertrag mit Palantir endet und nicht verlängert wird.

Diese Einschränkungen bedingen weder eine gesonderte vertragliche Vereinbarung mit Palantir noch zusätzliche Kosten. Die Nutzung von Künstlicher Intelligenz in der VeRA ist mit dem beauftragten Softwareprodukt „Gotham“ und der darin integrierten eingeschränkten Version des Softwareprodukts „Foundry“ grundsätzlich nicht möglich.

14. zu welchem Zeitpunkt insbesondere mit Blick auf die notwendigen Änderungen im Polizeigesetz sowie die Implementierung von Palantir die Landesregierung von einer tatsächlichen Nutzbarkeit ausgeht;

Zu 14.:

Die Planungen des PTLs Pol sehen derzeit vor, dass noch im Jahr 2025 die für den Betrieb der VeRA erforderlichen Hard- und Softwarekomponenten von Palantir bereitgestellt werden. Mit dem Abschluss der weiteren Maßnahmen zur Integration in die hessische IT-Infrastruktur und zur Anbindung an Baden-Württemberg wird Anfang 2026 gerechnet. Eine Wirkbetriebsaufnahme der VeRA ist für das 2. Quartal 2026 avisiert.

15. welche Software Frankreich und Interpol nach ihrer Kenntnis aktuell nutzen unter Darstellung, inwiefern der Landesregierung bekannt ist, ob sie Palantir bereits genutzt haben.

Zu 15.:

Der öffentlichen Presseberichterstattung zufolge wird die Software „Gotham“ von Palantir derzeit bei der französischen Direction Générale de la Sécurité Intérieure (DGSI) eingesetzt. Aktuell finden demnach jedoch auf mehrere Jahre ausgelegte Umstellungsarbeiten auf die Software „Outil de Traitement des Données Hétérogènes“ (OTDH), basierend auf der Software „ArgonOS“ der französischen Firma ChapsVision, statt. Es liegen jedoch keine Informationen vor, dass das Produkt „ArgonOS“ bereits in einer Behörde produktiv im Einsatz wäre. Der vorgenannten Presseberichterstattung ist zu entnehmen, dass bei der DGSI zwar ein Umstieg auf die Software des Anbieters ChapsVision erfolgen soll, dieser Umstieg jedoch auf mehrere Jahre ausgelegt ist und bis dahin weiter die Software „Gotham“ von Palantir genutzt werden soll.

Bei Interpol handelt es sich um eine Organisation, welche die Stärkung der Zusammenarbeit nationaler Polizeibehörden zum Ziel hat, und folglich keine operativen Aufgaben wahrnimmt. Es liegen keine Informationen zu bei Interpol (auch in der Vergangenheit) verwendeten Softwareprodukten vor.

Strobl

Minister des Inneren,
für Digitalisierung und Kommunen