SACHSEN-ANHALT
Ministerium für
Inneres und Sport

Ministerium für Inneres und Sport des Landes Sachsen-Anhalt
Postfach 3563 • 39010 Magdeburg

**Ministerin**

Präsident des Landtages
von Sachsen-Anhalt
Herrn Dr. Gunnar Schellenberger, MdL
Domplatz 6 - 9
39104 Magdeburg

12. Juni 2025

**Einführung einer automatisierten Datenanalyseplattform;**
**Kleine Anfrage der Abgeordneten Eva von Angern und Andreas Henke (Die Linke) – LT-Drs. KA 8/2983 vom 19. Mai 2025**

Sehr geehrter Herr Landtagspräsident,

beigefügt übersende ich Ihnen die Antwort der Landesregierung – erstellt vom Ministerium für Inneres und Sport – auf die o. g. Kleine Anfrage mit der Bitte um Kenntnisnahme.

Mit freundlichen Grüßen

Dr. Tamara Zieschang
Ministerin für Inneres und Sport

Anlage

35871/2025

Halberstädter Str. 2/
am „Platz des 17. Juni“
39112 Magdeburg

Telefon (0391) 567-5500
Telefax (0391) 567-5510
min@mi.sachsen-anhalt.de
www.mi.sachsen-anhalt.de

Landeshauptkasse Sachsen-Anhalt
Deutsche Bundesbank
BIC MARKDEF1810
IBAN DE21 8100 0000 0081 0015 00

**Antwort der Landesregierung auf eine Kleine Anfrage zur schriftlichen Beantwortung**

Abgeordnete Eva von Angern und Andreas Henke (Die Linke)

**Einführung einer automatisierten Datenanalyseplattform;**

Kleine Anfrage – **KA 8/2983**

**Vorbemerkung der Anfragesteller:**

*Datiert auf den 05.02.2025 brachte die Landesregierung gemeinsam mit dem Land Bayern einen Bundesratsantrag ein (Drs. 58/25), der den Titel trägt: „Priorisierung, auskömmliche Finanzierung und rechtssichere Implementierung eines gemeinsamen Datenhauses für die Informationsverarbeitung der Polizeien des Bundes und der Länder - Neuausrichtung polizeilicher IT (P20) sowie interimsweise zeitnahe Bereitstellung einer gemeinsam betriebenen automatisierten Datenanalyseplattform". Wie Ministerpräsident Haseloff in seiner Einbringungsrede am 14.02. erklärte, soll es mit diesem Entschließungsantrag darum gehen, „dass sich die Bundesregierung der drängenden Verantwortung für die umgehende Evaluierung und Optimierung der aktuellen Sicherheitsarchitektur stellt und zügig handelt, damit solche entsetzlichen Gewalttaten zukünftig besser abgewendet und vermieden werden können.*

**Antwort der Landesregierung erstellt vom Ministerium für Inneres und Sport**

**Vorbemerkung der Landesregierung:**

Aufgrund der Amokfahrt auf dem Weihnachtsmarkt in Magdeburg am 20. Dezember 2024 sowie im Zusammenhang mit der Gewährleistung der Sicherheit des Weihnachtsmarktes werden gegenwärtig mehrere strafrechtliche Ermittlungsverfahren geführt. Trotz der grundsätzlichen verfassungsrechtlichen Pflicht, Informationsansprüche des Landtages von Sachsen-Anhalt zu erfüllen, tritt hier nach sorgfältiger Abwägung der betroffenen Belange im Einzelfall das Informationsinteresse des Parlaments hinter dem berechtigten Geheimhaltungsinteresse zum Schutz der laufenden Ermittlungen zurück. Eine weitergehende Auskunft könnte in Teilen gegenwärtig andauernde Ermittlungsverfahren

erschweren oder gar gefährden. Aus dem Prinzip der Rechtsstaatlichkeit folgt daher, dass das betroffene Interesse der Allgemeinheit an der Gewährleistung einer funktionstüchtigen Strafrechtspflege und Strafverfolgung hier Vorrang vor dem parlamentarischen Informationsinteresse genießt. Bei parlamentarischen Anfragen, die ein laufendendes Ermittlungsverfahren tangieren, ist daher u. a. stets zu prüfen und abzuwägen, ob durch eine Auskunftserteilung gegebenenfalls der Ermittlungserfolg gefährdet oder gar vereitelt werden könnte. Seitens der Landesregierung wird zudem darauf hingewiesen, dass die Aufarbeitung der Amokfahrt auf dem Magdeburger Weihnachtsmarkt weiterhin andauert.

**Frage 1:**

***Welche Schlüsse hat die Landesregierung aus dem Anschlag in Magdeburg gezogen und auf welcher Grundlage passierte das?***

**Frage 2:**

***Wie hätte, nach Einschätzung der Landesregierung, mittels einer Analysesoftware der Anschlag in Magdeburg verhindert werden können, wie der Antrag für den Bundesrat vermittelt und welche weiteren Optionen zur Problemlösung wurden in Erwägung gezogen?***

**Antwort auf die Fragen 1 und 2:**

Die Fragen 1 und 2 werden zusammenhängend beantwortet.

Die Amokfahrt auf dem Magdeburger Weihnachtsmarkt am 20. Dezember 2024 ist neben der laufenden strafrechtlichen auch Gegenstand einer noch andauernden polizeifachlichen und parlamentarischen Aufarbeitung. Mithin sind abschließende Bewertungen und Schlussfolgerungen zum gegenwärtigen Zeitpunkt noch nicht sachgerecht möglich.
Bereits jetzt steht fest, dass der Landespolizei Sachsen-Anhalt vor der Amokfahrt nicht sämtliche Informationen von Bundesbehörden sowie dem Bundesministerium für Inneres und Heimat und dem Bundeskanzleramt sowie von Landespolizeien anderer Bundesländer zum Beschuldigten vorlagen. Daher hat das Land Sachsen-Anhalt eine Bundesratsinitiative initiiert, die insbesondere die Implementierung eines gemeinsamen Datenhauses für die Informationsverarbeitung der Polizeien des Bundes und der Länder vorsieht,

um den Austausch von Informationen der Sicherheitsbehörden untereinander zu verbessern und vergleichbare Taten künftig besser vermeiden zu können.

Im Übrigen wird auf die Vorbemerkung der Landesregierung verwiesen.

**Frage 3:**

***Im Antrag wird zwischen einer „mittelfristige Nutzung eines gemeinsamen Datenhauses" sowie einer „kurzfristigen, zentralen Bereitstellung einer gemeinsam betriebenen Datenanalyseplattform" unterschieden. Letztere soll in „einigen Landespolizeien schon im Einsatz" sein (Punkt 2, Drs. 58/25).***

**Frage 3a:**

***Wer ist für die Bereitstellung des hier benannten „gemeinsamen Datenhauses" zuständig?***

**Antwort auf Frage 3a:**

Das gemeinsame Datenhaus wird im Rahmen des Bund-Länder-Programms „Polizei 20/20 – Neuausrichtung polizeilicher IT (P20)" aufgebaut. Teilnehmer am Programm P20 sind alle Landespolizeien, die Bundespolizei, das Bundeskriminalamt, die Polizei des Deutschen Bundestages und das Zollkriminalamt. Hauptziel ist die Harmonisierung und Digitalisierung der heterogen gewachsenen polizeilichen IT-Infrastrukturen von Bund und Ländern. Kernziele des Programms P20 sind die Verbesserung der Verfügbarkeit polizeilicher Informationen, eine Erhöhung der Wirtschaftlichkeit sowie die Stärkung des Datenschutzes durch Technik.

**Frage 3b:**

***In welchem Zeitfenster soll dieses „gemeinsame Datenhaus" nutzbar werden?***

**Antwort auf Frage 3b:**

Zum Jahresende 2024 wurde die technische Bereitstellung und damit ein wichtiger Meilenstein für die Inbetriebnahme des Datenhauses erreicht. Sukzessive werden initiale Services durch erste Teilnehmer in den Wirkbetrieb genommen. Die 20 Teilnehmer werden zu unterschiedlichen Zeitpunkten die Services des Datenhauses nutzen, weshalb keine verbindliche Aussage hierzu getroffen werden kann.

Im Übrigen wird auf die Antwort auf Frage 3a verwiesen.

**Frage 3c:**

***Was soll dieses „gemeinsame Datenhaus" leisten?***

**Antwort auf Frage 3c:**

Das Datenhaus bildet das Kernelement des Programms P20. Es schafft einen zentralen Speicherort für die polizeilichen Daten der Polizeien von Bund und Ländern und trägt damit zur Umsetzung der Saarbrücker Agenda bei. Die Daten werden bei der Speicherung im Datenhaus in eigenen, voneinander getrennten Bereichen abgelegt, sodass jede Polizeibehörde die Datenhoheit über die von ihr erfassten Daten behält. Neben dem Datenhaus wird sukzessive das sogenannte Datenhaus-Ökosystem aufgebaut, welches Services der polizeilichen Sachbearbeitung integriert.

Im Übrigen wird auf die Antwort auf Frage 3a verwiesen.

**Frage 3d:**

***Welche der polizeilich genutzten Datenbanken und Anwendungen sollen im Zielbild Teil des „gemeinsamen Datenhauses" sein und welche Maßnahmen wurden zur Zielerreichung durch die Polizei Sachsen-Anhalt bereits umgesetzt oder eingeleitet?***

**Antwort auf Frage 3d:**

Im Zielbild werden neben den bestehenden Verbundsystemen bzw. -datenbanken auch die drei Vorgangsbearbeitungssysteme sowie die für die polizeiliche Sachbearbeitung notwendigen Services verstetigt sein. Dabei werden teilweise bestehende Anwendungen zielbildkonform ertüchtigt, aber auch neue Services etabliert. Zur Erreichung des Zielbildes werden die bisherigen dezentralen Systeme und Anwendungen durch zentrale Funktionen und Dienste abgelöst bzw. ersetzt. Der Zugriff auf die Daten im Datenhaus erfolgt nicht willkürlich, sondern folgt datenschutzrechtlichen Maßgaben.

Mit Blick auf die Zielbilderreichung des P20 hat die Landespolizei Sachsen-Anhalt zum Ende des Jahres 2024 als erster Programmteilnehmer sein polizeiliches Vorgangsbearbeitungssystem auf eines der drei (Interims-)Vorgangsbearbeitungssysteme (iVBS) umgestellt. Nach gegenwärtiger Beschlusslage sollen alle Programmteilnehmer über den

Weg der Migration auf ein iVBS die Transformation in das Zielbild und folglich den Anschluss an das Datenhaus gewährleisten.

Zudem ist die Polizei des Landes Sachsen-Anhalt bereits an das sogenannte „Föderale-Identity and Accessmanagement angebunden. Dessen sukzessive Weiterentwicklung sorgt dafür, dass sich Anwender aller Programmteilnehmer im Datenhaus bzw. den dortigen Fachanwendungen, Diensten und Services anmelden (authentifizieren) und über personenbezogene Zugriffsrechte autorisiert arbeiten können.
Die Maßnahmen und Aktivitäten der Landespolizei mit Bezug zum Programm P20 korrelieren mit den im Bund-Länder-Kontext abgestimmten übergreifenden Transformationsschritten und sind auf das Erreichen des gemeinsamen Zielbilds, dem Datenhausökosystem ausgerichtet.

Im Übrigen wird auf die Antwort auf Frage 3a verwiesen.

**Frage 3e:**

***Worin besteht für die Landesregierung der Mehrwert der kurzfristigen übergangsweisen Nutzung einer Datenanalyseplattform?***

**Antwort auf Frage 3e:**

Aufgrund der bisherigen Heterogenität der polizeilichen Datenhaltung in Bund und Ländern werden die polizeilich relevanten Daten einer polizeilichen Auswertung und Analyse über eine Vielzahl von Einzelabfragen nur schwer bis teilweise gar nicht zugeführt. Häufig liegen diese in den verschiedenen polizeilichen Quellverfahren dezentral und mehrfach vor, was dem datenschutzrechtlichen Grundsatz der Datensparsamkeit widerspricht. Insofern ist langfristiges Kernziel des Programms P20 durch die Implementierung eines gemeinsamen Datenhauses und einem differenzierten Rechte- und Zugriffsmanagement den Grundsatz des Datenschutzes durch Technik zu gewährleisten.
Aufgrund des bestehenden fachlichen Erfordernisses der Polizeien des Bundes und der Länder, in Fällen schwerster Kriminalität oder extremer Gefahrenlagen unverzügliche Suchen und Recherchen sowie Analysen durchführen zu können, ist bis zur Fertigstellung eines gemeinsamen Datenhauses eine übergangsweise Nutzung einer zentral betriebenen automatisierten Datenanalyseplattform eine geeignete Möglichkeit,

die Daten vollständig integriert in einer Plattform der polizeilichen Auswertung und Analyse zuzuführen.

**Frage 3f:**
***Welche Landespolizeien nutzen bereits eine solche Datenanalyseplattform?***

**Frage 3g:**
***Welche Software zur Datenanalyse kommt jeweils in den Bundesländern zum Einsatz und wer ist im Einzelnen jeweils Anbieter dieser Software?***

**Antwort auf die Frage 3f und 3g:**
Die Fragen 3f und 3g werden zusammenhängend beantwortet.

Die Landesregierung kann keine Auskünfte zur Planung, Implementierung und tatsächlichen Nutzung von polizeilichen IT-Produkten anderer Länder sowie zum Sachstand der dortigen landesinternen Einführung machen.

**Frage 3h:**
***Welche Daten werden bei der Analyse dieser Plattform verarbeitet und auf welche Datenbanken nimmt sie automatisiert Zugriff?***

**Antwort auf Frage 3h:**
Grundsätzlich ist es möglich, über Datenanalyseplattformen insbesondere Daten aus den polizeilichen Informationssystemen sowie Vorgangsdaten und Falldaten zusammenzuführen und zu verarbeiten.

**Frage 3i:**
***Auf welchen Servern werden die Daten gespeichert (Deutschland, Europa oder außerhalb von Europa)? Wenn außerhalb von Europa, wo konkret?***

**Frage 3j:**
***Haben der Anbieter der Software, deren Betreiber oder Dritte Zugriffsmöglichkeiten auf Daten, die bei Nutzung der Software anfallen (bitte aufgeschlüsselt nach Metadaten und Inhaltsdaten jeweils für die Datenspeicherung, Datenübertragung und Datenverarbeitung beantworten) und wenn ja, welche technischen und***

***vertraglichen Vorkehrungen sieht die Landesregierung als erforderlich an, um entsprechende Datenzugriffe zu unterbinden?***

**Antwort auf die Fragen 3i und 3j:**

Die Fragen 3i und 3 j werden zusammenhängend beantwortet.

Da bisher keine finale Entscheidung für eine zeitnahe, interimsweise Bereitstellung einer zentral betriebenen, digital souveränen, wirtschaftlich tragbaren und rechtlich zulässigen automatisierten Datenanalyseplattform für alle Polizeien des Bundes und der Länder getroffen wurde, kann zum Standort von Servern und der Datenspeicherung derzeit auch keine Auskunft gegeben werden.

**Frage 4:**

***Was konkret versteht die Landesregierung unter der im Antrag geforderten digitalen Souveränität der automatisierten Datenanalyseplattform?***

**Antwort auf Frage 4:**

Digitale Souveränität wird definiert als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können".[1] Dabei umfasst die Begrifflichkeit sowohl die technologische Souveränität als auch die Datensouveränität.

Sie zielt generell darauf ab, Unabhängigkeit von einzelnen Wirtschaftsräumen, (außereuropäischen) Staaten und Unternehmen bei Bezug und Nutzung digitaler Technologien, Dienste und Plattformen herzustellen sowie proprietäre Abhängigkeiten und sogenannte Anbieterbindungseffekte zu vermeiden. In diesem Zusammenhang fokussiert digitale Souveränität im Einzelnen auf:

(a) eigene Fähigkeiten zur Entwicklung, Herstellung und Veredelung digitaler Schlüsseltechnologien, Dienste und Plattformen;

(b) eigene Fähigkeiten zur Prüfung und Bewertung digitaler Technologien, Dienste und Plattformen unter Leistungs- und Sicherheitsaspekten;

(c) Fähigkeiten von Sicherheitsbehörden und Verwaltungen, digitale Technologien und Lösungen sicher, selbstständig und selbstbestimmt einzusetzen;

---

[1] Definition nach der Studie zum Thema „Digitale Souveränität" der Kompetenzstelle Öffentliche IT (ÖFIT).

(d) hoheitliche Handlungsfähigkeit des Staats zum Schutz von Vertraulichkeit, Verfügbarkeit und Integrität von Informationen und Kommunikation nach innen und außen.

**Frage 4a:**

***Handelt es sich bei der Anforderung der digitalen Souveränität nach Ansicht der Landesregierung um eine essenzielle Vertragsbedingung oder lediglich um eine Soll-Anforderung mit welchen Ausnahmen und Einschränkungen?***

**Antwort auf Frage 4a:**

Die in der Antwort auf Frage 4 aufgeführten Anforderungen werden als essenzielle Voraussetzung der vertraglichen Gestaltung gesehen.

**Frage 4b:**

***Schließt sich die Landesregierung dem Beschluss 2021/09 des IT-Planungsrats zur Digitalen Souveränität an, dass die strategischen Ziele Wechselfähigkeit, Gestaltungsfähigkeit und Einfluss auf IT-Anbieter beachtet werden müssen und wenn ja, wie soll und wird dies hinsichtlich der geplanten Beschaffung der Datenanalyse-Software in Sachsen-Anhalt konkret umgesetzt?***

**Antwort auf Frage 4b:**

Der Beschluss des IT-Planungsrates wird durch die Landesregierung geteilt. Das Verständnis der Sicherheitsbehörden geht jedoch aufgrund besonderer Schutzbedarfe sowie der Verfügbarkeit, Vertraulichkeit und Integrität der Daten im Bereich der Informationssicherheit und des Geheimschutzes sowie des Datenschutzes darüber hinaus. Mit der Bundesratsinitiative „Priorisierung, auskömmliche Finanzierung und rechtssichere Implementierung eines gemeinsamen Datenhauses für die Informationsverarbeitung der Polizeien des Bundes und der Länder - Neuausrichtung polizeilicher IT (P20) sowie interimsweise zeitnahe Bereitstellung einer gemeinsam betriebenen automatisierten Datenanalyseplattform“ (BR-Drs. 58/25) hatte die Landesregierung den Bund aufgefordert, eine gemeinsam finanzierte, zentral zu betreibende, rechtlich zulässige Interimslösung für eine automatisierte Datenanalyseplattform für Bund und Länder bereit zu stellen.

**Frage 4c:**

***Ist Betrieb und Wartung der Software durch einen Anbieter aus der EU, der nicht zu mehr als 24 Prozent unter Kontrolle von Drittstaat-Unternehmen ist, nach Ansicht der Landesregierung, eine Bedingung für digitale Souveränität?***

**Antwort auf Frage 4c:**

Mit Blick auf Betrieb und Wartung von digitalen Sicherheitsinfrastrukturen im Allgemeinen und konkreten Softwareprodukten im Besonderen muss gewährleistet werden, dass diese keinen strukturellen Einflussmöglichkeiten hinsichtlich Verfügbarkeit, Vertraulichkeit, Integrität und ihrer Rechtskonformität durch außereuropäische Staaten ausgesetzt sind. Im Übrigen wird auf die Antwort auf Frage 4 verwiesen.

**Frage 4d:**

***Ist Open-Source-Software nach Ansicht der Landesregierung, verglichen mit proprietärer Software, vorteilhaft für die digitale Souveränität, unabhängige Überprüfbarkeit der Funktionsweise der Software, Möglichkeit den Betreiber zu wechseln (Exit-Strategie), Möglichkeit die Software nach eigenem Ermessen weiterzuentwickeln und an eigene Bedürfnisse anzupassen, Sicherung des Datenschutzes und der IT-Sicherheit allgemein und wenn ja, wird Open-Source-Software entsprechend eine Anforderung in entsprechenden Ausschreibungen oder Vertragsverhandlungen sein und wenn nein, wie sollen die genannten Aspekte auch ohne Open-Source-Software sichergestellt werden?***

**Antwort auf Frage 4d:**

In Anlehnung an die Bundesratsinitiative (BR-Drs. 58/25) forciert Sachsen-Anhalt die interimsweise Bereitstellung einer zentral betriebenen, digital souveränen, wirtschaftlich tragbaren und rechtlich zulässigen automatisierten Datenanalyseplattform durch den Bund unabhängig von einem konkreten Produkt. Zur Frage, inwieweit – neben den fachlichen und betrieblichen Anforderungen – speziell die Nutzung von Open-Source-Software Gegenstand der entsprechenden Ausschreibungen oder Vertragsverhandlungen sein werden, liegen der Landesregierung – insbesondere unter Hinweis auf den in diesem Zusammenhang nicht abgeschlossenen Bund-Länder-Abstimmungsprozess – keine belastbaren Informationen vor.

Der Bund verfügt durch das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung gleichwohl über eine umfassende Expertise zur Sicherherstellung von digital souveränen Lösungen.

**Frage 4e:**

***Welche Schlüsse zieht die Landesregierung aus der Entscheidung der Bundesregierung vom Sommer 2023, die Einführung von Bundes-VeRA mit der Begründung zu stoppen, dass Ziele des P20-Programms die hersteller-unabhängige Anwendungsbereitstellung und der Betrieb von polizeilichen Funktionalitäten mit hoher Autonomie und flexibler Erweiterung und Anpassung seien (vgl. BT-Drs. 20/8390, Frage 2)?***

**Antwort auf Frage 4e:**

Die Schlussfolgerungen der Landesregierung sind mit der Bundesratsinitiative (BR-Drs. 58/25) und der Forderung der Einführung einer gemeinsam finanzierten, zentral zu betreibenden, rechtlich zulässigen und digital souveränen Interimslösung für eine automatisierte Datenanalyseplattform gezogen worden.

**Frage 5:**

***Was plant die Landesregierung, um eine Rechtsgrundlage für eine bundes- und europarechtlich zulässige, automatisierte Verarbeitung von Daten der Bürgerinnen und Bürger zu schaffen?***

**Antwort auf Frage 5:**

Die Landesregierung hat den Entwurf eines Elften Gesetzes zur Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) (LT-Drs. 8/5018) in den Landtag eingebracht. In diesem Gesetzentwurf ist eine Befugnis zur Durchführung operativer und strategischer Datenanalysen vorgesehen. Das Bundesverfassungsgericht hat in seinem Urteil vom 16. Februar 2023 zur automatisierten Datenanalyse (Az. 1 BvR 1547/19, 1 BvR 2634/20) die verfassungsrechtliche Legitimität von Befugnissen zur automatisierten Datenanalyse bestätigt und die verfassungsrechtlichen Anforderungen an entsprechende Vorschriften konkretisiert.

**Frage 6:**

***Wie sollen in der zu schaffenden Rechtsgrundlage nationale und unionsrechtliche Anforderungen an Datenschutz berücksichtigt werden und welche technisch-organisatorischen Maßnahmen sind für die Umsetzung bereits vorgesehen?***

**Antwort auf Frage 6:**

Zur Umsetzung der Richtlinie (EU) 2016/680 hat der Landtag von Sachsen-Anhalt im August 2019 das Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt (DSUG LSA) erlassen. Die Polizei hat dieses Gesetz bei der Verarbeitung personenbezogener Daten bei der Verhütung von Straftaten und straftatenbezogenen Gefahrenabwehr zu beachten (§ 13a Abs. 1 SOG LSA).

Im Übrigen wird auf die Antwort auf die Fragen 3i und 3j verwiesen.

**Frage 7:**

***Wie und welche Kontrollinstanz ist geplant, um zu gewährleisten, dass***

- ***a. unbefugte Dritte keinen Zugriff auf die Daten erhalten (Datensicherheit),***
- ***b. keine unnötigen oder unerlaubten Daten (z. B. Gesundheitsdaten) von Bürgerinnen und Bürgern erhoben werden (Datenschutz),***
- ***c. sich Bürgerinnen und Bürger bei Verstößen gegen den Datenschutz beschweren und ihre Rechte geltend machen können?***

**Antwort auf Frage 7a:**

Die Anforderungen an die Sicherheit der Datenverarbeitung bestimmen sich nach § 20 DSUG LSA. Danach haben die (datenschutzrechtlich) Verantwortlichen die Maßnahmen zur Datensicherheit nach einer Risikobewertung zu ergreifen. Zur Verwehrung des Zugangs zur Analyseplattform für Unbefugte (Zugangskontrolle) sieht der Gesetzentwurf eine Verordnungsermächtigung vor (§ 30a Abs. 8 Nr. 2). Nach § 24 Abs. 3 Satz 2 Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt (DSAG LSA) ist die Landesbeauftragte für den Datenschutz vor dem Erlass von Rechtsvorschriften, die den Umgang mit personenbezogenen Daten betreffen, zu hören.

**Antwort auf Frage 7b:**

Die geplante Befugnis ermächtigt die Polizei ausschließlich, rechtmäßig gespeicherte Daten zum Zweck der Durchführung operativer oder strategischer Datenanalysen auf einer Analyseplattform automatisiert zusammenzuführen und bei Vorliegen bestimmter

Tatbestandsvoraussetzungen weiterzuverarbeiten. Der geplante § 30a SOG LSA ermächtigt nicht, personenbezogene Daten zu erheben.

**Antwort auf Frage 7c:**

Die Rechte der betroffenen Personen bestimmen sich, soweit nach dem SOG LSA keine speziellen Regelungen getroffen worden sind (vergleiche § 32a und § 32c SOG LSA), nach dem Kapitel 3 DSUG LSA. Die Vorschriften des Abschnitts 5 „Datenschutzbeauftragter" des DSAG LSA gelten bei Aufgaben der Datenschutzbeauftragten im Anwendungsbereich der Richtlinie (EU) 2016/680 bei öffentlichen Stellen, die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit zuständig sind, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Damit obliegt der Landesbeauftragten für den Datenschutz die Überwachung der Einhaltung der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften.

**Frage 8:**

***Welche in Punkt 7 des Antrags genannten Regelungslücken sieht die Landesregierung innerhalb der Strafprozessordnung für den „Einsatz des späteren gemeinsamen Datenhauses sowie einer automatisierten Datenanalyse für den repressiven Bereich"?***

**Antwort auf Frage 8:**

Der Bundesratsinitiative (BR-Drs. 58/25) ist eine Ziffer 7 nicht zu entnehmen. Mithin geht die Landesregierung davon aus, dass die Frage Bezug auf Ziffer 6 der Bundesratsinitiative nimmt. Das Bundesverfassungsgericht hat in seinem Urteil vom 16. Februar 2023 ausdrücklich darauf hingewiesen, dass die automatisierte Datenanalyse grundsätzlich verfassungsrechtlich zu rechtfertigen und damit zulässig sein kann. Dies erfordere jedoch die Schaffung spezialgesetzlicher Rechtsgrundlagen in den jeweiligen Polizeigesetzen. Die rechtlichen Auswirkungen des Urteils wurden im Programm Polizei 20/20 bewertet. Obgleich die Strafprozessordnung (StPO) nicht Prüfungsgegenstand des vorbenannten Urteils war, wurde im Ergebnis die Schaffung einer Rechtsgrundlage in der StPO grundsätzlich befürwortet, um den fachlichen Mehrwert einer Analyseplattform auch zu repressiven Zwecken vollständig ausschöpfen

zu können und einen rechtskonformen Einsatz zu legitimieren. Hiermit würde zudem den verfassungsrechtlichen Grundsätzen nach Rechtsstaatlichkeit, Bestimmtheit und Verhältnismäßigkeit genüge getan.

**Frage 9:**

***Wer und wie werden die bereinigten Datensätze für den „Einsatz des späteren gemeinsamen Datenhauses sowie einer automatisierten Datenanalyse für den repressiven Bereich" erstellt (siehe Empfehlung Landesdatenschutzbeauftragte LSA im INN am 24.04.2025)?***

**Antwort auf Frage 9:**

Finalisierte fachliche, technische und (datenschutz-)rechtliche Dokumentationen zur Beschreibung von Rechten und Rollen, detaillierten Zugriffsberechtigungen sowie technischen Datenverarbeitungsprozessen sowohl für den Einsatz des späteren gemeinsamen Datenhauses als auch einer automatisierten Datenanalyse liegen noch nicht vor, finden aber grundsätzlich im Rahmen der Einführung neuer IT-Anwendungen Berücksichtigung.

Die Einbeziehung der jeweils zuständigen Datenschutzbeauftragten des Bundes und der Länder erfolgt standardmäßig im Rahmen etablierter Verfahrenswege. In diesem Zusammenhang wird auf § 24 Abs. 3 Satz 2 DSAG LSA verwiesen. Im Zuge der dort festgeschriebenen Unterrichtung des bzw. der Landesbeauftragte(n) für den Datenschutz werden die Einhaltung datenschutzrechtlicher Standards zum Aufbau und zur Änderung von automatisierten Verfahren zur Verarbeitung von personenbezogenen Daten gewährleistet.

**Frage 10:**

***Ist geplant, die Daten im Zusammenhang der Nutzung der Software zum Schutz vor unbefugten Zugriffen verschlüsselt zu verarbeiten, übertragen und zu speichern (bitte jeweils getrennt beantworten)?***

**Antwort auf Frage 10:**

Die Frage der Sicherstellung der Informationssicherheit, des Geheimschutzes und der Vertraulichkeit und Integrität der Daten im Rahmen des Datenschutzes hat bei den Sicherheitsbehörden einen hohen Stellenwert. Auch im Rahmen der Implementierung

einer automatisierten Datenanalyseplattform sind in Abhängigkeit eines landesinternen Eigenbetriebs oder eines Fremdbetriebs (bspw. bei dem Landesdienstleister Dataport AöR bzw. dem Bundeskriminalamt selbst) Verschlüsselungsmechanismen des Transportes und Ende-zu-Ende vorgesehen. Diese werden in Abhängigkeit einer grundlegenden Entscheidung zu einem zentralen Betrieb durch Bund und Länder zu einem späteren Zeitpunkt spezifiziert.

**Frage 11:**

***Mit welchen technischen Mitteln plant die Landesregierung problematische Einfallstore wie etwa Cloud-Nutzung oder Fernwartung bei einer Datenanalysesoftware auszuschließen?***

**Antwort auf Frage 11:**

Die Nutzung von Cloud-Technologien und Fernwartung wird nicht per se als problematisch angesehen. Insbesondere der Aufbau eigener (Private-)Cloud-Infrastrukturen bei den Sicherheitsbehörden oder bei öffentlichen Dienstleistern unter Nutzung von modernen Verschlüsselungstechnologie sind Herausforderungen, denen sich die Sicherheitsbehörden in Bund und Ländern derzeitig stellen. Es muss gleichwohl sichergestellt werden, dass insbesondere die Fähigkeit der automatisierten Datenanalyse als ein Schlüsselelement der künftigen digitalen Sicherheitsinfrastruktur hinsichtlich Verfügbarkeit, Vertraulichkeit, Integrität und ihrer Rechtskonformität gewährleistet ist.