**Antrag 2025/KL/3**
**AGS RLP**

**Empfehlung der Antragskommission**
**Annahme in der Version der Antragskommission**

**Keine Beschaffung oder Nutzung von Softwareprodukten des Unternehmens Palantir Technologies Inc. durch Polizei- und Sicherheitsbehörden des Landes Rheinland-Pfalz**

Der Landesparteitag möge beschließen:
1. Die Landesregierung wird aufgefordert, sicherzustellen, dass Polizei- und Sicherheitsbehörden des Landes Rheinland-Pfalz keine Softwarelösungen der Palantir Technologies Inc. (insbesondere „Gotham“ oder vergleichbare Analyseplattformen) beschaffen, testen oder dauerhaft einsetzen.
2. Bereits beschaffte Produkte sollen zeitnah stillgelegt werden.
3. Die Landesregierung wird aufgefordert, sicherzustellen, dass sämtliche Daten aller Polizei- und Sicherheitsbehörden des Landes Rheinland-Pfalz ausschließlich auf Servern und Verarbeitungsplattformen gespeichert und verarbeitet werden, die keiner Behörde, Gerichten oder Entscheidern außerhalb des Rechtes und der Jurisdiktion des Landes, des Bundes bzw. der EU Einsicht oder Zugriff ermöglichen.
4. Die Landesregierung wirkt im Rahmen ihrer Möglichkeiten darauf hin, dass auch auf Bundesebene und in anderen Bundesländern derartige Softwareprodukte ausgeschlossen werden, sofern sie gegen Grundrechte, europäische Datenschutzvorgaben oder rechtsstaatliche Prinzipien verstoßen.

**Begründung**
1. Verstoß gegen europäisches Datenschutzrecht (DSGVO) und KI-Regulierung
Die Nutzung von Palantir-Produkten durch deutsche Polizeibehörden wirft erhebliche datenschutzrechtliche Bedenken auf:

Ab Zeile 21 Ergänzung durch

5. Wir erkennen den Nutzen von Analyseplattformen für die Arbeit der Strafverfolgungsbehörden im 21. Jahrhundert. Insbesondere Frankreich ist hierbei europaweit bei der Einführung eigener Lösungen führend. Auch wir fordern für Deutschland eigene Lösungen, auch im Sinne digitaler Souveränität. Die Landesregierung soll sich deshalb bundesweit für die Forschung und Entwicklung einer vergleichbaren Analyseplattform einsetzen, mit der Polizist:innen unterstützt werden und gleichzeitig sicher sind, dass unsere Daten nicht in falsche Hände gelangen.

• Palantir ist ein US-amerikanisches Unternehmen, das unter den „Foreign Intelligence Surveillance Act“ (FISA, insbesondere Section 702) fällt. Somit kann die US-Regierung ohne Wissen der Betroffenen auf die gespeicherten Daten zugreifen – auch bei Nutzung in Europa.
• Die DSGVO (Art. 44– 49) untersagt eine Datenverarbeitung durch Unternehmen, die nicht garantieren können, dass europäische Datenschutzrechte eingehalten werden. Kein Unternehmen, dass sich mehrheitlich in US-Besitz befindet oder deren Verbindungsknoten oder Speicher sich auf US-Territorium befinden, kann dieses garantieren.
• Mit dem Inkrafttreten des KI-Gesetzes (AI Act) der EU gelten strenge Anforderungen für den Einsatz hochriskanter Systeme im Bereich der öffentlichen Sicherheit. Die Systeme von Palantir sind – auch nach Einschätzung europäischer Juristen – intransparent, nicht auditierbar und nicht konform mit europäischer KI-Governance.

2. Demokratische Kontrolle, Transparenz und Neutralität von IT-Partnern Ein demokratischer Rechtsstaat muss bei sensibler IT-Infrastruktur wie Polizeisoftware besonders sorgfältig darauf achten, wem er welche Infrastruktur und Machtmittel anvertraut. Palantir wurde mit massiver Anschubfinanzierung der CIA-nahe gegründeten Organisation In-Q-Tel aufgebaut und ist nicht neutral:
• Einer der Gründer und Hauptaktionäre, Peter Thiel, ist ein radikal-libertärer Milliardär, der sich offen gegen demokratische Institutionen stellt (u. a. mit dem Zitat: „I no longer believe that freedom and democracy

are compatible.“)
• Palantir war und ist eng in militärische und geheimdienstliche Operationen involviert – etwa in Afghanistan, bei ICE-Abschiebungen in den USA oder in geheimen Predictive-Policing-Projekten.
• Das Unternehmen verweigert durchgehend die Offenlegung seiner Algorithmen, Datenmodelle und Bias-Prüfungen. Die demokratische Polizei in Rheinland-Pfalz sollte weder technologisch abhängig werden von einem Konzern mit totalitär-affiner Gesinnung, noch darf sie den Zugriff auf die sensiblen Daten ihrer Bürgerinnen und Bürger einem Unternehmen mit zweifelhaften internationalen Verflechtungen anvertrauen.

3. Lehren aus der deutschen Geschichte: Keine unkontrollierbaren „Superdatenbanken“ für potenzielle „Superbehörden“ Dieser Aspekt gewinnt besonders im Lichte zunehmender Einflussmöglichkeiten rechter Parteien mit fragwürdiger Verfassungstreue und anzunehmender nationalsozialistischer bzw. faschistischer Grundlage an Bedeutung. Wenn schon der Bundestag unlängst die Hürden für die Richterwahl für das BVG et al präventiv höher gehängt hat, um derartigen Einflüssen vorzubeugen, zeigt es, dass man sich auf der Ebene der Entscheider dieser Gefahr durchaus bewusst ist. In der nationalsozialistischen Diktatur war die systematische Erfassung, Kategorisierung und Vernetzung personenbezogener Daten eine tragende Säule der Verfolgung, Unterdrückung und Ermordung von Millionen Menschen. Die Zusammenarbeit von Verwaltung, Polizei und Geheimdiensten mit Zugriff auf zentrale

Aktenbestände führte zur Effizienzsteigerung der Unfreiheit. Aus dieser historischen Erfahrung leitet sich für das demokratische Deutschland das Prinzip ab, Datenbestände zu dezentralisieren, Zugriff zu begrenzen und informationelle Gewaltenteilung sicherzustellen.

Der Einsatz von Systemen wie Palantir Gotham, das massenhafte Datenbanken verknüpft und „präventiv“ Muster erkennt, führt exakt zu einer solchen Superdatenbankstruktur mit Behörden übergreifender Zugriffsmöglichkeit. Dies widerspricht den historischen Lehren und unserer verfassungsrechtlich verankerten demokratischen Sicherheitsarchitektur.

Zusammenfassung: Der Einsatz von Palantir-Software widerspricht:

- den Grundsätzen der Gewaltenteilung,
- der DSGVO,
- dem europäischen AI Act,
- den demokratischen Anforderungen an Transparenz, Rechenschaftspflicht und staatliche Souveränität,
- sowie den Lehren aus der NS-Vergangenheit über zentrale Datenmacht,

Rheinland-Pfalz sollte als demokratisches Bundesland mit Vorbildfunktion bei digitaler Ethik, Bürgerrechten und Open-Source-Strategie bewusst auf den Einsatz von Palantir-Produkten verzichten und stattdessen auf transparente, quelloffene, auditierbare Lösungen setzen, wie sie z. B. im Rahmen von EU-Förderprogrammen (z. B. GAIA-X) entwickelt werden.

Bereits angeschaffte Produkte sollten zeitnah stillgelegt werden.