

HÄUFIG GESTELLTE FRAGEN

US-Geheimdienstoperationen · Palantir Gotham in Baden-Württemberg

Datensouveränität · Air-Gap-Sicherheit · Die Ausstiegsfrage 2030

Verifiziert Juli 2026 · Alle Aussagen mit Primärquellen belegt

FAQ 1 Welches sind die bedeutendsten dokumentierten Fälle von US-Geheimdienstoperationen gegen EU-Mitgliedstaaten und deren Institutionen?

Kurze Antwort: Es gibt eine lange und verifizierte Dokumentation von US-Geheimdienstoperationen gegen EU-Regierungen, Staatsoberhäupter, Botschaften und Unternehmen – darunter Deutschland und Frankreich. Es handelt sich nicht um Vorwürfe: Der Großteil ist durch NSA-Dokumente, parlamentarische Anfragen und Gerichtsverfahren belegt.

Operation	Ziele	Zeitraum	Verifizierte Quelle
ECHELON (NSA/GCHQ gemeinsam)	Regierungen, Industrie, Diplomatie – UK, Frankreich, Deutschland u.a.	1971–heute	NSA-Dokumente/The Intercept; EU-Parlamentsbericht 2001
PRISM / TEMPORA	Massenerfassung von Internet- & Telefondaten; UK als Partner und Ziel	2007–2013	Snowden-Enthüllungen; The Guardian (Jun 2013)
NSA-Massenüberwachung – Deutschland	~500 Millionen Telefonate, E-Mails & SMS pro Monat	2012–2013	Der Spiegel; Snowden-Dokumente
Abhören der Handys Merkel & Schröder	Persönliche Mobiltelefone der Bundeskanzler	2002–2013	Der Spiegel; The Guardian; CBS News
Abhören französischer Staatspräsidenten	Präsidenten Chirac, Sarkozy und Hollande	2006–2012	WikiLeaks; Libération; Mediapart (2015)
Verzanzen von EU-Botschaften (Op. 'Perdido')	38 Botschaften & UN-Vertretungen; verschlüsseltes Fax der franz. EU-Botschaft	~2010+	The Guardian; Snowden-NSA-Dokumente
NSA NCEUR – Stuttgart-Vaihingen	NSA-Europazentrale (Einheit F202); Zweck offiziell unbekannt	2008–heute	Bundesinnenministerium (2013); electrospace.net
AFRICOM-Drohneinsätze – Stuttgart	Planung tödlicher Angriffe in Afrika über Kelley Barracks	2008–heute	ECCHR; Lawfare; OVG Münster 2019; BVerfG 2025

► Quelle: EU-Parlamentsbericht 2001 (STOA) · NSA/The Intercept · Snowden/The Guardian Jun 2013 · Der Spiegel 2013 · WikiLeaks 2015 · ECCHR ecchr.eu · OVG Münster 19. März 2019 · BVerfG-Pressemitteilung Jul 2025 (bvg25-059) · Bundesinnenministerium, Antwort auf parlamentarische Anfrage von MdB Ute Vogt (2013)

„Europa muss bei der Software-Entwicklung aufholen und souveräner werden.

Das ist von strategischer Bedeutung in Zeiten, in denen sich die geopolitische Tektonik verschiebt.“

— Innenminister Thomas Strobl BW, 29. Juli 2025

✓ VERIFIZIERTE QUELLENANGABEN

[1] EU-Parlament STOA-Bericht (2001): 'Entwicklung von Überwachungstechnologien und Risiken des Missbrauchs von Wirtschaftsinformationen' — www.europarl.europa.eu/doceo/document/A-5-2001-0264_EN.html

[2] Snowden, E. (Jun 2013): PRISM- und TEMPORA-Folien an The Guardian übermittelt – NSA/GCHQ-Massenerfassung bestätigt — theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[4] Der Spiegel (Okt 2013): 'NSA überwacht 500 Millionen Verbindungen in Deutschland pro Monat' – auf Basis von Snowden-Dokumenten — [NSA überwacht 500 Millionen Verbindungen in Deutschland - DER SPIEGEL](#)

[5] Der Spiegel (Okt 2013): 'Handy-Überwachung: NSA belauschte Merkels Handy seit 2002' – durch NSA-Dokumente bestätigt — [spiegel.de/politik/deutschland/nsa-belauschte-angela-merkel-schon-seit-2002-a-929642.html](#)

[6] WikiLeaks / Libération / Mediapart (Jun 2015): NSA-Dokumente bestätigen Abhören von Chirac, Sarkozy und Hollande (2006–2012) — [wikileaks.org/nsa-france](#)

[7] [National Security Agency – Wikipedia](#) - Existenz der NSA NCEUR auf den Patch Barracks

[8] [Trumps zweite Amtszeit bringt neue US-Militärstrategie für Afrika](#) - Africom

[9] ECCHR (2019–2025): Klagen zu Drohneneinsätzen — [ECCHR: Italy's responsibility in deadly US drone strike in Libya](#)

[10] Innenminister Strobil BW, Pressekonferenz 29. Juli 2025 – 'Europa muss bei der Software-Entwicklung aufholen' — [stm.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/ermittlungsbehoerden-erhalten-neue-instrumente](#)

FAQ 2 Welche strukturellen Rechtsanomalien und Grauzonen bestehen konkret auf deutschem und baden-württembergischem Boden?

Kurze Antwort: Drei aktive strukturelle Anomalien – NCEUR, AFRICOM und die Exposition gegenüber FISA/Cloud Act – schaffen Grauzonen, in denen US-Geheimdienst- und Militäraktivitäten auf deutschem Boden unter Bedingungen stattfinden, die deutsches Recht nicht vollständig erfassen kann.

2.1 NSA-Europazentrale (NCEUR) auf den Patch Barracks, Stuttgart-Vaihingen

Aspekt	Verifizierter Befund
Offizieller Name	NSA/CSS Representative Europe Office (NCEUR) – interner Code F202; benachbarte Einheit F204 = Geheimdienstunterstützung für AFRICOM
Standort	Patch Barracks, Stuttgart-Vaihingen (mit EUCOM und SOCEUR kolosiert)
Rechtliche Grundlage bestätigt durch	Bundesinnenministerium, parlamentarische Antwort an SPD-MdB Ute Vogt (2013) – Existenz bestätigt; keine weiteren Angaben
Zweck	Offiziell unbekannt. Weder die Bundesregierung noch die Investigativjournalisten Fuchs & Goetz (Geheimer Krieg, Rowohlt 2013) konnten klären, was die Dienststelle tut
Grauzone	Kein deutsches Kontrollgremium ist zuständig; Aktivitäten sind eingestuft; die Dienststelle operiert unter US-Militärgerichtsbarkeit auf deutschem Boden

► Quelle: Bundesinnenministerium 2013 · [electrospaces.net](#) · Fuchs/Goetz 'Geheimer Krieg' (Rowohlt 2013) · Kontext Wochenzeitung 2013 · Stuttgarter Nachrichten 2013

2.2 AFRICOM – US Africa Command auf den Kelley Barracks, Stuttgart-Möhringen

Aspekt	Verifizierter Befund
Funktion	Hauptquartier für alle US-Militäroperationen in Afrika (50+ Länder) – einschließlich der Planung von Drohnenanschlägen in Jemen, Somalia, Libyen und Mali; Erstellung von 'Kill Lists'; Nominierung von Zielpersonen für tödliche Aktionen
Stationierung	Oktober 2008 – in Stuttgart platziert, weil kein afrikanisches Land die Aufnahme akzeptierte
Fragen des deutschen Rechts	GG Art. 2 Abs. 2: Das OVG Münster (2019) stellte fest, Deutschland habe eine Verfassungspflicht, US-Operationen von seinem Territorium aus zu kontrollieren. GG Art. 26 Abs. 1: Kritiker argumentieren, Drohnenkriege ohne UN-Mandat stellten eine verfassungswidrige Vorbereitung eines Angriffskrieges dar
Gerichtsgeschichte	2015: VG Köln bestätigte extraterritoriale Anwendbarkeit von Art. 2 GG; 2019: OVG Münster fand 'gewichtige Anhaltspunkte' für IHL-Verstöße in Jemen; 2020: BVerwG Leipzig hob das OVG-Urteil auf; 2025: BVerfG wies die Verfassungsbeschwerde ab – keine systematischen Verstöße nachgewiesen
NATO-SOFA-Grenze	Kritiker argumentieren, das NATO-Truppenstatut ermächtige Deutschland nicht, Kommandostrukturen zu beherbergen, die zur Planung offensiver tödlicher Operationen außerhalb eines erklärten Krieges genutzt werden

► Quelle: ECCHR ([ecchr.eu](#)) · [Lawfaremedia.org](#) · OVG Münster, Urteil 19. März 2019 · BVerfG-Pressemitteilung Jul 2025 (bvg25-059) · Open Society Justice Initiative · IKRK-Fallsammlung · [Columbia Journal of Transnational Law](#)

2.3 FISA 702 und der Cloud Act – Strukturelle Exposition aller US-Technologie auf deutschem Boden

Cloud Act (2018): Verpflichtet US-Unternehmen, Daten auf Anfrage an US-Behörden herauszugeben – unabhängig davon, wo die Daten physisch gespeichert sind, ohne Gerichtsbeschluss und ohne Benachrichtigung der betroffenen Person. Ein Microsoft-Manager sagte am 17. Juli 2025 unter Eid in Frankreich aus, dass grundsätzlich nicht garantiert werden könne, dass keine Daten an US-Behörden weitergegeben werden.

FISA Section 702 (50 U.S.C. §1881a): Ermächtigt die NSA, US-Unternehmen ohne richterlichen Beschluss zur Unterstützung bei der Auslandsaufklärung zu zwingen – ohne dass der ausländische Kunde (wie die BW-Polizei) informiert wird. Wiederbewilligt April 2024 (RISAA) bis April 2026, dann erneut verlängert.

National Security Letters (NSLs): Das FBI kann US-Unternehmen zur Herausgabe von Unterlagen zwingen und ihnen gleichzeitig untersagen, den Empfang der Anfrage offenzulegen. Deutschland hat über NSLs keine Hoheitsgewalt. Der deutsche Auftraggeber würde nicht informiert.

Wesentliche Konsequenz: Palantir Technologies Inc. ist ein US-Unternehmen. Alle genannten US-Rechtsinstrumente gelten für das Unternehmen. Der Standort des Rechenzentrums in Deutschland hebt die US-rechtlichen Verpflichtungen des Unternehmens nicht auf. Keine Vertragsklausel zwischen BW-Polizei und Palantir kann die Pflichten überschreiben, die Palantir gegenüber der US-Regierung hat.

„Einmal mehr wurde bestätigt, dass die Verpflichtung zur Datenweitergabe nach dem Cloud Act für alle US-Unternehmen gilt.

Das macht eine europäische Lösung umso dringlicher – insbesondere für den Einsatz von Diensten durch Regierungen,

Behörden, sonstige öffentliche Stellen und Betreiber kritischer Infrastrukturen.“

— Kirsten Bock, Stiftung Datenschutz

Am 3. Juni 2026 verabschiedete die Europäische Kommission ein Maßnahmenpaket zur Stärkung der technologischen Souveränität.

In besonders sensiblen Bereichen – wie der Polizeiarbeit – soll künftig nur noch europäische Software und Hardware zulässig sein.

EU-Kommissarin Virkkunen warnte vor der Gefahr eines 'Kill Switch', den ausländische Regierungen betätigen könnten,

um unsere digitale Infrastruktur abzuschalten.

► Quelle: Cloud Act (2018, 18 U.S.C. §2713) · FISA §702 (50 U.S.C. §1881a) – RISAA-Wiederbewilligung Apr 2024 · Brennan Center for Justice, FISA 702 Ressourcenseite 2026 · stateofsurveillance.org · Microsoft-Aussage Frankreich, 17. Jul 2025 · EU-Kommission Digitalpaket Souveränität, 3. Jun 2026 · Rede Kommissarin Virkkunen Jun 2026

✓ VERIFIZIERTE QUELLENANGABEN

[1] Fuchs, A. / Goetz, J.: 'Geheimer Krieg – Wie von Deutschland aus der Drohnenkrieg gesteuert wird' (Rowohlt, 2013) – Zweck von NCEUR auch nach Recherchen unklar

[2] Lawfaremedia.org: 'German Courts Weigh Legal Responsibility for US Drone Strikes' (Jan 2023) — lawfaremedia.org/article/german-courts-weigh-legal-responsibility-us-drone-strikes

[3] Cloud Act (2018), 18 U.S.C. §2713 – Pflicht US-amerikanischer Unternehmen zur Datenweitergabe an US-Behörden unabhängig vom Speicherort

FISA Section 702 (50 U.S.C. §1881a) — [Section 702 of the Foreign Intelligence Surveillance Act, Explained | Brennan Center for Justice](#)

[4] CLOUD Act und der Patriot Act - [Keine Garantien: Microsoft muss EU-Daten an USA übermitteln | heise online](#)

[5] Europäische Kommission, Digitalpaket Technologische Souveränität, 3. Juni 2026 – Einschränkung auf europäische Software/Hardware für sensible öffentliche Bereiche — ec.europa.eu/commission/presscorner/detail/en/ip_26_1187

[6] Rede Kommissarin Virkkunen, Juni 2026 – Warnung vor ausländischem 'Kill Switch' für europäische digitale Infrastruktur - [EU aims to ensure foreign governments or firms cannot disrupt tech services with 'kill switch' | European Commission | The Guardian](#)

FAQ 3 Was ist das offiziell erklärte Ziel der Einführung von Palantir Gotham in BW – und zu was ist Palantir Gotham im Vollbetrieb tatsächlich in der Lage?

Kurze Antwort: Die Landesregierung BW hat einen engen polizeirechtlichen Anwendungsfall einer Plattform lizenziert, die für militärische und nachrichtendienstliche Operationen im Vollspektrum konzipiert wurde. Viele Fähigkeiten, die nicht beantragt – und offiziell ausgeschlossen – wurden, sind dennoch im System vorhanden und in anderen Einsatzszenarien aktiv.

Fähigkeitsbereich	BW beantragt offiziell	Vollständige Gotham-Fähigkeit	Lücke / Überschuss
Kernanwendung	Verfahrensübergreifende Suche & Verknüpfung von Daten aus polizeilichen Datenbanken zur Terrorismusbekämpfung und Verhinderung schwerer Straftaten	Durchgängige Geheimdienstanalyseplattform für Verteidigung, Nachrichtendienste und Strafverfolgung bei allen Five-Eyes-Nationen und NATO-Mitgliedern	BW lizenziert einen engen präventivpolizeilichen Teilbereich einer Plattform für den militärischen Vollspektrumsbetrieb
Datenintegration	Verknüpfung isolierter interner Polizeidatenbanken (Strafakten, Verbindungsdaten, sichergestellte Geräte)	Alle strukturierten oder unstrukturierten Datenquellen über dynamische Ontologie; Echtzeit-Verbund mit externen Systemen und Live-Sensor-Feeds	Gotham kann sich mit eingestufteten Systemen und Drohnen-/Satelliten-Live-Feeds verbinden – nicht nur mit internen Polizeidateien
Netzwerkanalyse	Erkennung von Verbindungen zwischen Personen, Orten und Ereignissen	Zentrale Zielidentifikation und Visualisierung der 'Befehlshierarchie'; unterstützt militärisches Kill-Chain-Management	Dieselbe Graph-Engine, die zur Verbindung von Tatverdächtigen genutzt wird, dient der Erstellung militärischer Zielanschlagspakete
KI / Maschinelles Lernen	Zunächst ausgeschlossen (erklärt)	KI erkennt Muster, verbessert die Bedrohungserkennung und automatisiert komplexe Analysen; Palantir/NVIDIA (29. Jun 2026): Telemetriedaten trainieren sich selbst verbessernde Missionsmodelle	§57a PolG öffnet gleichzeitig Polizeidaten für das KI-Training – die rechtliche Tür steht offen, auch wenn der operative Einsatz 'ausgeschlossen' ist
Prädiktive Analyse	In keiner offiziellen BW-Kommunikation erwähnt	Dokumentierter Einsatz für predictive policing (LAPD, eingestellt 2019); ICE FALCON prognostiziert das Untertauchen von Arbeitnehmern vor Razzien	Prädiktives individuelles Scoring ist ein aktiver Anwendungsfall in anderen Rechtsordnungen auf derselben Plattformversion
Kill Chain / Zielerfassung	Explizit nicht Bestandteil jeglicher BW-Kommunikation	Gotham unterstützt eine 'KI-gestützte Kill Chain' – nahtlose Zielidentifikation und Waffenzuweisung; gilt als prägend für die Kriegsführung in der Ukraine via Drohnen-zu-Kill-Chain-KI	Die an die BW-Polizei lizenzierte Plattform ist dieselbe, die für tödliche Zielentscheidungen eingesetzt wird
SIGINT-Integration	Explizit ausgeschlossen (§47a PolG)	Konsolidiert OSINT, SIGINT, Überwachungs- und Aufklärungsdaten in einem einheitlichen Lagebild	SIGINT-Integration ist eine architektonische Kernfähigkeit – der Ausschluss beruht auf Konfiguration, nicht auf Architektur
Prüfung und Kontrolle	Parlamentarisches Kontrollgremium tagt 4x jährlich (nichtöffentlich)	Palantirs eigenes CIRT überwacht die Plattform rund um die Uhr in Echtzeit; alle Nutzerinteraktionen werden	Palantir hat einen umfassenderen Echtzeitzugang zum System als das parlamentarische Kontrollgremium

Fähigkeitsbereich	BW beantragt offiziell	Vollständige Gotham-Fähigkeit	Lücke / Überschuss
		von Palantir-Infrastruktur protokolliert	
Ausstieg / Interoperabilität	Als 5-jährige Brückentechnologie geplant; Ablösung bis 2030	Palantir-Systeme sind nicht mit anderen Produkten interoperabel; selbst erzeugte Abhängigkeit ist in Hessen und NRW nach jahrelangem Einsatz dokumentiert	Die Bezeichnung 'Brückentechnologie' widerspricht der strukturellen Abhängigkeit, die Palantirs Ontologie-Modell erzeugt

► Quelle: BW Staatsministerium, Pressemitteilung 29. Jul 2025 · Landtag BW 17/9329 (Aug 2025) · Palantir UK Government Digital Marketplace Service Definition 2024 · Palantir 10-K GJ2020 (SEC EDGAR) · Palantir/NVIDIA Business Wire 29. Jun 2026 · netzpolitik.org Nov 2025 · heise.de Nov 2025

⚠ WESENTLICHER BEFUND	BW hat die unteren Etagen eines Gebäudes lizenziert, das weitere Stockwerke hat – vollständig ausgebaut und bei anderen Kunden aktiv genutzt –, deren Zugang ausschließlich durch Konfiguration, nicht durch Architektur beschränkt wird. Palantirs eigene Ingenieure halten den Generalschlüssel für Wartungszwecke.
------------------------------	---

✓ VERIFIZIERTE QUELLENANGABEN
[1] BW Staatsministerium, Pressemitteilung 29. Juli 2025: offiziell erklärter Zweck von VeRA – Terrorismusbekämpfung, verfahrensübergreifende Suche — stm.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/ermittlungsbehoerden-erhalten-neue-instrumente
[2] Landtag BW, Drucksache 17/9329 (August 2025): parlamentarische Anfrage – Regierungsposition zu Palantir VeRA, Rechenzentrumsstandort, Mitarbeiterzugang
[3] Palantir UK Government Digital Marketplace, Service Definition (2024): vollständige Gotham-Fähigkeitsbeschreibung einschließlich Verteidigungs-, Geheimdienstkontroll- und Targeting-Funktionen
[4] Palantir Technologies 10-K GJ2020 (SEC EDGAR): Modell der Forward Deployed Engineers – 'FDEs have travelled to bases in Afghanistan... to deploy our platforms' — sec.gov/cgi-bin/browse-edgar?action=getcompany&CIK=PLTR
[5] Palantir / NVIDIA Business Wire, 29. Juni 2026: 'Intelligent engine collects and stores user telemetry and trace data, then uses that data to post-train and align the model' — businesswire.com/news/home/20260629390275/en
[6] netzpolitik.org, 13. November 2025: 'Grüne geben Polizeidaten für Palantir frei' – Kill-Chain- und SIGINT-Fähigkeiten dokumentiert — netzpolitik.org/2025/gruene-geben-polizeidaten-fuer-palantir-frei/
[7] heise.de, 12. November 2025: 'Baden-Württemberg entscheidet sich für Einsatz von Palantir' – KI-Ausschluss und parlamentarische Kontrolldetails — Trotz Überrumpelung: Baden-Württemberg stimmt für Palantir heise online
[8] netzpolitik.org, 10. November 2025: LAPD Predictive Policing (eingestellt 2019) und ICE FALCON – dokumentierter Einsatz derselben Plattform zur prädiktiven Einzelpersonenbewertung

FAQ 4 Warum sind die vereinbarten Schutzmaßnahmen strukturell unzureichend – sowohl im Normalbetrieb als auch dann, wenn Palantir eine rechtsverbindliche US-Regierungsanordnung erhält?

Kurze Antwort: Die Schutzmaßnahmen beruhen auf Palantirs Selbstkontrolle, schließen unabhängige technische Prüfungen aus und können das US-Recht nicht außer Kraft setzen. Die Sicherheitsüberprüfung prüft Identität, nicht staatsangeordnete Compliance. Die Experimentierklausel (§57a PolG) schafft einen formal legalen Datentransferkanal, der die vertraglichen Schutzmaßnahmen vollständig umgeht.

Ebene / Risiko	Offizielle Position	Status	Verifizierte Bewertung
Daten auf deutschen Servern	✓ Bestätigt (Landtag 17/9329)	EINGESCHRÄNKT	Verifiziert – aber rechtlich irrelevant, sobald §57a Experimentierklausel die Übermittlung personenbezogener Polizeidaten an private Unternehmen für KI-Entwicklung und -Tests erlaubt
Kein Fernexport von Daten möglich	✓ Behauptet (17/9329)	NICHT VERIFIZIERBAR	Kann ohne unabhängige technische Prüfung nicht verifiziert werden. Palantirs eigenes CIRT überwacht die Mitarbeiter in Echtzeit – keine externe Drittkontrolle des laufenden BW-Betriebs (heise.de, Nov 2025)
Sicherheitsüberprüfung Palantir-Personal	✓ Sicherheitsüberprüfung bestätigt	UNZUREICHEND	Überprüfung prüft Identität und Hintergrund. Sie verhindert NICHT den staatlich angeordneten Zugriff via FISA/NSL; auch ein compliant agierender Insider wäre durch die firmeneigene Überwachung nicht erkennbar. Präzedenzfälle: Snowden, Manning und Reality Winner waren alle vollständig überprüft
Schutz vor US-rechtlichem Zwang (FISA/NSL)	✗ Im Vertrag und PolG nicht adressiert	BLINDER FLECK	Palantir ist ein US-Unternehmen. FISA 702 ermächtigt die NSA, ohne richterlichen Beschluss Unterstützung für Auslandsaufklärung anzuordnen. NSLs enthalten Schweigegebote – die BW-Polizei würde nicht informiert. Deutschland hat über diese US-Rechtsinstrumente keinerlei Jurisdiktion
§57a Experimentierklausel	⚠ Rechtlich zulässig (PolG BW, 12. Nov 2025)	OFFENES TOR	§57a ermächtigt ausdrücklich zur Übermittlung personenbezogener Polizeidaten an 'nichtöffentliche Stellen' (= Privatunternehmen) für KI-Training, -Tests und -Validierung. netzpolitik.org: 'Ein Dammbruch – Daten wurden nie für diesen Zweck erhoben; einmal als Trainingsdaten in KI-Modellen, praktisch nicht mehr zurückzuholen'
Air-Gap- / Covert-Channel-Risiko	In keinem offiziellen Dokument erwähnt	NICHT ADRESSIERT	Mehr als 30 begutachtete Angriffsmethoden (RAMBO 2024, PIXHELL 2024) belegen, dass Air-Gapped-Netzwerke nicht absolut sicher sind, sobald ein compliant agierender Insider mit Wartungszugang anwesend ist. Ein Palantir-FDE-Besuch = klassischer Stuxnet-artiger initialer Angriffsvektor
Unabhängige technische Prüfung im laufenden Betrieb	✗ Fehlt	FEHLEND	Weder BW noch ein anderes deutsches Bundesland hat unabhängigen Stellen im laufenden Betrieb eine Prüfung von Palantir ermöglicht. GFF-Verfassungsklage läuft. Das parlamentarische Kontrollgremium tagt 4x jährlich in nichtöffentlicher Sitzung – es führt keine technischen Audits durch

► Quelle: Landtag BW 17/9329 (Aug 2025) · §57a PolG BW (12. Nov 2025) · Landtag BW 17/9478 (Sep 2025) · heise.de 12. Nov 2025 · netzpolitik.org 13. Nov 2025 · Brennan Center FISA 702 (2026) · stateofsurveillance.org · Guri, RAMBO arXiv:2409.02292 · Guri, PIXHELL IEEE COMPSAC 2024 · Sensors 2023 MDPI DOI 10.3390/s23063215 · GFF freiheitsrechte.org · DoControl (2025) · Palantir Trust Portal safebase.us

X STRUKTURELLER BLINDER FLECK

Werden die Daten nicht sicher auf einem Server in Deutschland gespeichert? + Ja. Das ändert aber nichts, wenn Palantir eine FISA-Anordnung oder ein NSL erhält – das Unternehmen ist rechtlich zur Erfüllung verpflichtet, rechtlich daran gehindert, die BW-Polizei zu informieren, und der physische Standort der Daten in Deutschland hebt die US-rechtlichen Verpflichtungen des Unternehmens nicht auf.

✓ VERIFIZIERTE QUELLENANGABEN

- [1] Landtag BW, Drucksache 17/9329 (August 2025): Regierungsposition – kein unbeaufsichtigter Zugang, Daten auf deutschen Servern, alle Mitarbeiter sicherheitsüberprüft
- [2] §57a PolG BW (in Kraft seit 12. November 2025): Experimentierklausel – Übermittlung personenbezogener Polizeidaten an nichtöffentliche Stellen für KI-Training rechtlich zulässig — landesrecht-bw.de
- [3] Landtag BW, Drucksache 17/9478 (September 2025): Begründung zu §57a – Kosten 'derzeit noch nicht bezifferbar'; 'KI-Anwendungen benötigen realitätsnahe, polizeispezifische personenbezogene Trainingsdaten'
- [4] heise.de, 16. Juli 2025: Über Risiken beim Einsatz von Palantir - Verfassungsrechtler Jonas Botta — heise.de
- [5] netzpolitik.org, 13. November 2025: '§57a – ein Dammbruch; Daten wurden nie für diesen Zweck erhoben; einmal als KI-Trainingsdaten, praktisch nicht mehr rückholbar'
- [6] Brennan Center for Justice, FISA 702 Ressourcenseite 2026: Zwangsbefugnis der NSA; Schweigegebotsmechanismus bei NSLs – Deutschland hat keine Jurisdiktion — brennancenter.org
- [7] stateofsurveillance.org: 'US FISA 702 and Surveillance Laws 2026' – FISA-, Cloud-Act- und NSL-Exposition für US-Unternehmen in der EU — stateofsurveillance.org
- [8] Guri, M. et al.: RAMBO – 'Radiation of Air-gapped Memory Bus for Offense' (arXiv:2409.02292, NordSec 2023) – EM-Exfiltration über RAM-Bus im Labor bestätigt
- [9] Guri, M.: PIXHELL (IEEE COMPSAC 2024 / arXiv:2409.04930) – LCD-Pixelmuster erzeugen 0–22-kHz-Spulen-/Kondensator-Rauschen; Datenexfiltration ohne Audiohardware
- [10] Sensors 2023, 23(6):3215, MDPI: 'Survey on Air-Gap Attacks' – systematische Übersicht über 30+ Covert-Channel-Methoden (DOI: 10.3390/s23063215) — mdpi.com/1424-8220/23/6/3215
- [11] Palantir Trust Portal (safebase.us): Pipeline-Builder-Sicherheitsfehler – Object Security Policies werden bei Neuauslieferung lautlos gelöscht; Daten können für unbefugte Nutzer sichtbar werden
- [12] GFF – Gesellschaft für Freiheitsrechte: Verfassungsbeschwerden gegen Palantir in Bayern (2025); BW-Einsatz unter Beobachtung — freiheitsrechte.org
- [13] DoControl (2025): 'Palantir former employees steal company data via Slack' – Insider-Bedrohung bei Palantir selbst dokumentiert; Sicherheitsüberprüfung verhindert keine Insider-Compliance

FAQ 5 Darf Palantir BW-Polizeidaten zum Training seiner KI nutzen – und bestätigt Palantirs eigene Systemarchitektur, dass dieses Training stattfinden wird?

Kurze Antwort: Ja, in beiden Punkten, mit einer wichtigen Nuancierung: Das Recht erlaubt es; Palantirs Architektur ist dafür konzipiert; die vertragliche Aussage lautet, das trainierte Modell verbleibe in der Infrastruktur der BW-Polizei und stehe in deren Eigentum – dies kann jedoch nicht unabhängig verifiziert werden.

5.1 Was das Gesetz besagt – §57a PolG BW (in Kraft seit 12. November 2025)

§57a schafft eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten für die **Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von IT-Produkten einschließlich KI-Systemen und KI-Modellen** (im Sinne der EU-KI-Verordnung) – unabhängig von der Durchführung wissenschaftlicher Forschungsarbeiten. (Quelle: Landtag BW 17/9478, Sep 2025 – die amtliche Begründung des Gesetzes)

§57a Abs. 2 erlaubt die **Übermittlung dieser personenbezogenen Daten an nichtöffentliche Stellen** – nach deutschem Datenschutzrecht bedeutet 'nichtöffentliche Stellen' Privatunternehmen –, sofern die Empfänger zur Verschwiegenheit verpflichtet sind.

Eigene Begründung des Innenministeriums: „KI-Anwendungen benötigen zur Entwicklung und zum Testen realitätsnahe Trainingsdaten. Dazu brauche man die Nutzung polizeispezifischer – in aller Regel auch personenbezogener – Daten eben.“

Kosten aus §57a: 'Derzeit noch nicht bezifferbar' – laut amtlicher Folgenabschätzung (Beteiligungsportal BW, Haushaltsdokumente, Sep 2025).

5.2 Was Palantirs Architektur bestätigt – Palantir/NVIDIA-Ankündigung, 29. Juni 2026

Palantir kündigte am 29. Juni 2026 (Business Wire) eine strategische Initiative mit NVIDIA an, um eine Intelligent Engine zum Training und Einsatz von Modellen in souveränen Umgebungen bereitzustellen. Die Ankündigung besagt:

"The intelligent engine collects and stores user telemetry and trace data, then uses that data to post-train and align the model to areas where AI can add the most value. With this feedback loop, the model continually improves at supporting specific operational tasks."

— Palantir/NVIDIA Business Wire, 29. Juni 2026

WESENTLICHE NUANCIERUNG – Eigentümerschaft der trainierten Modellgewichte:

Die Ankündigung hält fest: *"Customers will own self-improving models specific to their mission."* Palantirs vertragliche Aussage lautet, die trainierten Modellgewichte verblieben in der eigenen Infrastruktur der BW-Polizei – die BW-Polizei erhält also eine sich selbst verbessernde KI, nicht Palantirs globales System.

Frage	Antwort	Belegt durch
Erlaubt §57a PolG rechtlich die Nutzung von BW-Polizeidaten für KI-Training?	JA – ausdrücklich	§57a PolG BW · Landtag BW 17/9478 (Sep 2025)
Ist Palantirs Plattform architektonisch für das Training von Modellen auf Nutzerdaten ausgelegt?	JA – Telemetrie- und Trace-Daten-Schleife bestätigt	Palantir/NVIDIA Business Wire 29. Jun 2026
Wem gehört das resultierende trainierte Modell?	BW-Polizei (vertraglich beansprucht)	Palantir/NVIDIA Business Wire 29. Jun 2026
Kann diese Aussage unabhängig verifiziert werden?	NEIN – keine unabhängige Prüfung im laufenden Betrieb vorhanden	heise.de Nov 2025 · Palantir Trust Portal safebase.us
Haben Betroffene (Verdächtige, Zeugen, Opfer) in die Nutzung für KI-Training eingewilligt?	NEIN – Daten wurden zu polizeilichen Zwecken erhoben, nicht für kommerzielle KI-Entwicklung	DSGVO Art. 5 Abs. 1 lit. b (Zweckbindung) · netzpolitik.org Nov 2025

Frage	Antwort	Belegt durch
Ist der Vorgang umkehrbar, sobald Daten in das KI-Training eingegangen sind?	NEIN – 'einmal als Trainingsdaten in KI-Modellen, praktisch nicht mehr rückholbar'	netzpolitik.org 13. Nov 2025 · CCC Stuttgart Stellungnahme Aug 2025

► Quelle: §57a PolG BW ([dejure.org / landesrecht-bw.de](https://www.dejure.org/länder/bw/landesrecht-bw.de)) · Landtag BW 17/9478 (Sep 2025) · IM BW Pressemitteilung 12. Nov 2025 ([im.baden-wuerttemberg.de](https://www.im.baden-wuerttemberg.de)) · Palantir/NVIDIA Business Wire 29. Jun 2026 ([businesswire.com](https://www.businesswire.com)) · netzpolitik.org 10. & 13. Nov 2025 · CCC Stuttgart Stellungnahme Aug 2025 ([cccs.de](https://www.cccs.de)) · Palantir Trust Portal (safebase.us)

✓ VERIFIZIERTE QUELLENANGABEN

- [1] §57a PolG BW (in Kraft seit 12. November 2025): Gesetzeswortlaut – KI-Training mit personenbezogenen Polizeidaten zulässig, Übermittlung an Privatunternehmen möglich — landesrecht-bw.de/bsbw/document/jlr-PolGBW2021pP57a
- [2] Landtag BW, Drucksache 17/9478 (September 2025): Begründung zu §57a – Wortlaut 'KI-Systeme und KI-Modelle im Sinne der KI-VO'; Kosten noch nicht bezifferbar
- [3] Innenministerium BW, Pressemitteilung 12. November 2025: 'Rechtsgrundlage zur Verarbeitung von Daten bei der Entwicklung, dem Training, dem Testen, der Validierung und der Beobachtung von IT-Produkten einschließlich KI-Systemen' — im.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/landtag-beschliesst-neufassung-des-polizeigesetzes
- [4] Palantir / NVIDIA Business Wire, 29. Juni 2026: 'Customers will own self-improving models specific to their mission. The intelligent engine collects and stores user telemetry and trace data, then uses that data to post-train and align the model' — [businesswire.com/news/home/20260629390275/en](https://www.businesswire.com/news/home/20260629390275/en)
- [5] Yahoo Finance / gurufocus, 29. Juni 2026: Palantir/NVIDIA – 'data does not migrate into closed model weights'; vertragliche Eigentumsanspruch des Kunden bestätigt — finance.yahoo.com/technology/ai/articles/palantir-nvidia-bring-open-ai-175410986.html
- [6] Palantir Trust Portal (safebase.us): Pipeline-Builder-Sicherheitsfehler – Object Security Policies werden bei Neuauslieferung lautlos gelöscht; Daten könnten für unbefugte Nutzer sichtbar werden
- [7] heise.de, 12. November 2025: 'Die Software konnte auch nach Jahren des Einsatzes von unabhängigen Stellen im laufenden Betrieb nicht geprüft werden' — [heise.de](https://www.heise.de)
- [8] netzpolitik.org, 13. November 2025: 'Einmal als Trainingsdaten beispielsweise in KI-Sprachmodelle eingegangen, sind die Daten kaum rückholbar'
- [9] CCC Stuttgart (CCCS), Stellungnahme August 2025: 'Es gibt keine klaren Anforderungen oder Beschränkungen für den KI-Einsatz; die Transparenz- und Kontrollbestimmungen sind unzureichend' — [cccs.de/2025-08-19-stellungnahme-polg-analyseplattform](https://www.cccs.de/2025-08-19-stellungnahme-polg-analyseplattform)
- [10] DSGVO Art. 5 Abs. 1 lit. b (Zweckbindung): Zu Polizeizwecken erhobene personenbezogene Daten können ohne eigenständige Rechtsgrundlage nicht für kommerzielle KI-Entwicklung umgewidmet werden

FAQ 6 Sind die Voraussetzungen erfüllt, damit ein europäisches Nachfolgeprodukt die erforderlichen Aufgaben bis 2030 auf demselben Stand erfüllen kann, den Palantir bis dahin erreicht haben wird?

Kurze Antwort: Nein. Es gibt keinen Entwicklungsvertrag, kein Entwicklungsbudget und keinen Prototypen. Auf Basis des einzigen realen Benchmarks (DGSi Frankreich, 6 Jahre von Programmstart bis Einsatz) hat BW den letzten vertretbaren Starttermin für 2030 bereits um mehr als 2 Jahre überschritten.

6.1 Der einzige reale Benchmark: die DGSi Frankreich (2016–2027)

Meilenstein	Datum	Was geschah
DGSi übernimmt Palantir Gotham	Dez 2016	Notfalleinsatz nach den Pariser Anschlägen (Nov 2015)
Ausschreibung OTDH-Nachfolgeprogramm	2021	Französisches Programm zur Ablösung von Palantir durch eine Eigenlösung gestartet
ChapsVision für OTDH vorausgewählt	2023	ChapsVision als bevorzugter Kandidat identifiziert
ChapsVision gewinnt Los 1 (Datenvorbereitung)	Ende 2024	Erste Phase vergeben – nur Verarbeitungsschicht
DGSi verlängert Palantir-Vertrag	Dez 2025	Eigenlösung noch nicht einsatzbereit; 3-jährige Verlängerung unterzeichnet
ChapsVision gewinnt Los 2 (Analysekern)	Juni 2026	Bekanntgegeben; vollständiger Einsatz für 2027 erwartet
→ Gesamtprogrammdauer	2021–2027	6 Jahre von Programmstart bis Betriebsbereitschaft einer Palantir-Entsprechung

► Quelle: TNW 16. Jun 2026 · L'informaticien 16. Jun 2026 · ChapsVision Wikipedia (fr) · The Wald Brief Mai 2026

6.2 Stand europäischer Alternativprodukte (Juli 2026)

Produkt	Herkunft	Status (Jul 2026)	Eignung für BW-Anwendungsfall
ChapsVision ArgonOS	Frankreich	DGSi Los 2 gewonnen Jun 2026; Einsatz 2027. Dt. Verfassungsschutz wählte es Mai 2026.	Ausgereifteste Option; fehlt militärische Kill-Chain; polizeirechtlich am nächsten
DataWalk	Polen	Bei EU/US-Sicherheitsbehörden im Einsatz; als direkte Gotham-Alternative vermarktet	Deckt Kern-Graphanalyse ab; kleineres KI-Trainings-Ökosystem als Palantir
Thales Artemis	Frankreich	DGSi-Ausschreibung verloren; als 'industrielles und politisches Desaster' bezeichnet; >120 Mio. € bis 2024 ausgegeben	Nur militärische KI; für polizeiliche Ermittlungsanalyse nicht geeignet
Europa-VeRA (BW-Konzept)	Deutschland	Bekanntgegeben Jul 2025: genannte Partner Airbus D&S + Schwarz Digits. Kein Vertrag, kein Prototyp, kein Budget (Jul 2026).	Geschätzte 7–10 Jahre bis Betriebsbereitschaft – auf Basis des französischen Benchmarks

► Quelle: The Wald Brief Mai 2026 · datawalk.com · Statewatch Okt 2025 · BW Staatsministerium 29. Jul 2025 · Schwarz Digits Wikipedia · TNW Jun 2026

6.3 Status Europa-VeRA: drei Fragen, drei verifizierte Antworten

Frage	Antwort	Belege
Wurde ein Entwicklungsauftrag erteilt?	NEIN	Nur eine Kooperationsankündigung (29. Jul 2025), in der Airbus D&S und Schwarz Digits als 'initiale Projektpartner' genannt

Frage	Antwort	Belege
		werden. Kein veröffentlichter Vertrag, keine Ausschreibung, keine Spezifikation, kein formales Projektteam (BW Staatsministerium; Koalitionsvertrag 2026).
Gibt es ein Entwicklungsbudget oder einen Landesfinanzierungsplan?	NEIN	Kein Haushaltsansatz im Staatshaushaltsplan BW 2025/2026 für die Entwicklung einer Alternative – nur 9,25 Mio. €/Jahr für den Betrieb von Palantir etatisiert. §57a-Kosten 'derzeit noch nicht bezifferbar'. Landtags-Entscheidung vom 12. Nov 2025 ist eine politische Handlungsaufforderung ohne jeglichen Mittelantrag. Keine EU-Horizon- oder Digital-Europe-Förderung angekündigt (Beteiligungsportal BW).
Ist eine sofortige Finanzierung erforderlich, um 2030 fertig zu sein?	JA – DRINGEND: bereits 2+ Jahre zu spät	Für ein 2030-Ziel hätten Entwicklungsverträge spätestens Ende 2024 unterzeichnet werden müssen – auf Basis des 6-Jahres-Benchmarks Frankreich. Ein im Januar 2027 gestartetes Programm könnte bestenfalls im Januar 2033 fertig sein. Bis 2030 wird Palantir 4 Jahre BW-Polizei-KI-Trainingsdaten in seinen Modellen eingebettet haben, gegen die jede Nachfolgelösung von null starten muss.

► Quelle: BW Staatsministerium 29. Jul 2025 (stm.bw.de) · Landtag BW Plenarprotokoll 12. Nov 2025 · Koalitionsvertrag Grün-Schwarz BW Mai 2026 (stuttgart-zeitung.de) · Beteiligungsportal BW Folgenabschätzung Sep 2025 · Schwarz Digits Wikipedia · netzpolitik.org 2026 · TNW Jun 2026 · Staatsanzeiger.de Nov 2025

✓ VERIFIZIERTE QUELLENANGABEN

- [1] Politico: 'France's DGSI drops Palantir Gotham in favour of ChapsVision ArgonOS' — [French spy service drops Palantir – POLITICO](#)
- [2] L'informaticien, 16. Juni 2026: DGSI wechselt zu ChapsVision Los 2 – vollständiger Einsatz 2027 erwartet (6 Jahre nach Programmstart 2021)
- [3] The Wald Brief, Mai 2026 (Gilles Delafon): Thales Artemis – 'industrielles und politisches Desaster'; >120 Mio. € ausgegeben; DGSI-Ausschreibung an ChapsVision verloren
- [4] datawalk.com: DataWalk-Produktbeschreibung – als direkte Palantir-Gotham-Alternative vermarktet; bei EU/US-Sicherheitsbehörden im Einsatz — datawalk.com/solutions/intelligence
- [5] BW Staatsministerium, Pressemitteilung 29. Juli 2025: Europa-VerA – 'Initiale Projektpartner sind die Airbus Defence and Space GmbH und die Digitalsparte der Schwarz Gruppe, Schwarz Digits' — stm.baden-wuerttemberg.de/de/startseite
- [6] Koalitionsvertrag Grün-Schwarz BW 2026 (Stuttgarter Zeitung, Mai 2026): 'bis spätestens 2030 eine Alternative zu Palantir entwickelt werden, die Datenhoheit sicherstellt' — stuttgart-zeitung.de
- [7] Landtag BW, Plenarprotokoll 12. November 2025: Entschließungsantrag von beiden Fraktionsvorsitzenden unterzeichnet – 'aktiv und intensiv' darauf hinwirken, dass EU-Alternative bis 2030 bereitsteht; kein Mittelantrag
- [8] Beteiligungsportal BW, Folgenabschätzung (September 2025): §57a-Kosten 'derzeit noch nicht bezifferbar'; nur 9,25 Mio. €/Jahr für Palantir-Betrieb im Staatshaushaltsplan 2025/2026 etatisiert — beteiligungsportal.baden-wuerttemberg.de/de/mitmachen/lp-17/polizeigesetz
- [9] Schwarz Digits Wikipedia (Stand April 2026): Geschäftsschwerpunkte bestätigt als STACKIT-Cloud, XM-Cyber-Cybersicherheit, Rechenzentrumserweiterung – NICHT Polizeianalysesoftware — en.wikipedia.org/wiki/Schwarz_Digits
- [10] netzpolitik.org, Juni 2026: 'Grüne: Palantir nein, Datenanalyse ja' – CDU BW und Grüne BW beide zum Ausstieg 2030 verpflichtet, aber noch kein Vertrag; Grünen-Mitgliederbefragung für sofortigen Abbruch läuft — netzpolitik.org/2026/gruene-palantir-nein-datenanalyse-ja
- [11] Staatsanzeiger.de, November 2025: 'Palantir-Einsatz wird auf fünf Jahre begrenzt' – Fünf-Jahres-Befristung im Koalitionskompromiss bestätigt — staatsanzeiger.de/nachrichten/politik-und-verwaltung/palantir-einsatz-wird-auf-fuenf-jahre-begrenzt

FAQ 7 Wie lautet das Gesamtrisikourteil – und was würde eine angemessene Aufsicht tatsächlich erfordern?

Risikodimension	Aktueller Stand	Urteil
US-Rechtszwang (FISA 702 / NSL / Cloud Act)	Im BW-Vertrag und PoIG BW nicht adressiert	✗ NICHT MITIGIERT – keine Vertragsklausel kann US-Bundesrecht außer Kraft setzen
§57a Experimentierklausel – Datenweitergabe	Seit 12. Nov 2025 rechtlich zulässig	✗ OFFEN – Polizeidaten können ohne unabhängige Kontrolle an Privatunternehmen für KI-Training fließen
Air-Gap- / Covert-Channel-Angriffsvektoren	In keinem offiziellen BW-Dokument erwähnt	✗ NICHT ADRESSIERT – 30+ erprobte Methoden; FDE-Wartungsbesuche = klassischer initialer Angriffsvektor
Palantir-Fähigkeitsüberschuss gegenüber erklärtem Zweck	Vertraglich eingeschränkt; architektonisch vorhanden	⚠ NUR KONFIGURATION – Militärfähigkeiten vorhanden; Ausschluss beruht auf Einstellungen, nicht auf Architektur
Unabhängige technische Prüfung	In BW und allen anderen deutschen Einsätzen fehlend	✗ FEHLEND – Palantirs eigenes CIRT hat mehr Echtzeitzugang zum System als das parlamentarische Kontrollgremium
Europa-VerA-Ausstieg bis 2030	Genannte Partner; kein Vertrag, kein Budget	✗ AUF KURS ZUM SCHEITERN – 2+ Jahre hinter dem auf dem franz. Benchmark basierenden Mindest-Starttermin
Demokratische Legitimität des Vertrags	Vom CDU-Innenministerium ohne Kenntnis des Koalitionspartners unterzeichnet	⚠ UMSTRITTEN – Grünen-Mitgliederbefragung für sofortigen Abbruch; neuer Koalitionsvertrag bekräftigt Ausstiegsziel 2030

7.1 Was eine angemessene Aufsicht erfordern würde

- 1. Unabhängige technische Prüfung – jetzt.** Eine technische Stelle mit vollem Systemzugang (nicht nur parlamentarischen Briefings) muss in der Lage sein, Datenflüsse, Modelltraining und Zugriffsprotokolle in Echtzeit im laufenden Betrieb zu verifizieren. Das aktuelle Modell – Palantir prüft sich selbst – ist strukturell unzureichend.
- 2. Öffentliche Offenlegung des Vertrags.** Der Palantir-Vertrag ist als VS-NfD eingestuft. IFG-Anfragen wurden abgelehnt. Keine demokratische Kontrolle der spezifischen technischen Zusagen ist möglich, solange der Vertragstext geheim bleibt.
- 3. Sofortiger Start der Europa-VerA – mit Vertrag und Budget.** Das Ziel 2030 erfordert spätestens Q4 2026 unterzeichnete Entwicklungsverträge. Genannte Partner und politische Entschlüsse sind kein Programm. Die Erfahrung der DGSi Frankreich (6 Jahre, 40 Mio. €, zwei gescheiterte Runden vor dem Erfolg) ist der Ausgangspunkt, nicht der günstigste Fall.
- 4. Rechtsgutachten zur FISA/Cloud-Act-Exposition.** BW hat keine rechtliche Einschätzung veröffentlicht, was geschieht, wenn Palantir eine US-Regierungsanordnung erhält. Dies ist das bedeutendste nicht adressierte strukturelle Risiko des gesamten Einsatzes.
- 5. Interim: Datenweitergaben nach §57a aussetzen.** Bis eine europäische Alternative betriebsbereit und eine unabhängige Prüfung eingerichtet ist, sollten Datenweitergaben an Privatunternehmen im Rahmen der Experimentierklausel ausgesetzt werden. Zu Polizeizwecken erhobene Daten dürfen ohne ausdrückliche, informierte Einwilligung nicht für kommerzielles KI-Training umgewidmet werden – eine Einwilligung, die für vor Bekanntwerden des Verwendungszwecks erhobene Daten nicht eingeholt werden kann.

„Wir wollen auf eine einsatzbereite Alternative umsteigen – so schnell wie möglich und spätestens bis 2030.“
— Grüne BW Landtagsfraktion, 12. November 2025

Es gibt derzeit keinen Vertrag, kein Budget und keinen Prototypen für diese Alternative.

Daher: Die Frist 2030 wird nicht eingehalten, wenn 2026 keine sofortigen Maßnahmen ergriffen werden.

Vollständiges Quellenverzeichnis

Kategorie	Verifizierte Primärquellen
BW-Polizeirecht & Palantir-Vertrag	§57a PolG BW · Landtag BW 17/9329 (Aug 2025) · Landtag BW 17/9478 (Sep 2025) · IM BW Pressemitteilung 12. Nov 2025 · Plenarprotokoll 12. Nov 2025 · Beteiligungsportal BW · Grüne BW Fraktion (gruene-landtag-bw.de) · netzpolitik.org · heise.de · kuketz-blog.de · abgeordnetenwatch.de · fragenstaat.de
Palantir-Architektur & Sicherheit	Palantir 10-K GJ2020 (SEC EDGAR) · Palantir/NVIDIA Business Wire 29. Jun 2026 · Palantir Trust Portal (safebase.us) · Palantir UK Gov Digital Marketplace Service Definition 2024 · DoControl (2025)
US-Rechtsrahmen	Cloud Act (18 U.S.C. §2713) · FISA §702 (50 U.S.C. §1881a) · RISAA-Wiederbewilligung Apr 2024 · Brennan Center FISA 702 Ressourcenseite 2026 · stateofsurveillance.org · ABA FISA 702 Ressourcen · Microsoft-Aussage Frankreich 17. Jul 2025
Air-Gap- & Covert-Channel-Forschung	Sensors 2023 MDPI DOI 10.3390/s23063215 · Guri RAMBO arXiv:2409.02292 · Guri PIXHELL IEEE COMPSAC 2024 · Guri AIR-FI IEEE TDSC 2023 · covertchannels.com · IBM Cost of a Data Breach 2025 · Mandiant M-Trends 2026
NSA Stuttgart & AFRICOM	Bundesinnenministerium, Antwort MdB Ute Vogt (2013) · electrospace.net · Fuchs/Goetz 'Geheimer Krieg' (Rowohlt 2013) · ECCHR ecchr.eu · lawfaremedia.org · OVG Münster 19. März 2019 · BVerfG-Pressemitteilung Jul 2025 (bvg25-059)
Europäische Alternativen & DGSi	TNW 16. Jun 2026 · L'informaticien 16. Jun 2026 · The Wald Brief Mai 2026 · ChapsVision Wikipedia (fr) · datawalk.com · Statewatch Okt 2025 · BW Staatsministerium 29. Jul 2025 · Koalitionsvertrag Grün-Schwarz BW 2026 · Staatsanzeiger.de · Schwarz Digits Wikipedia
US-Geheimdienstoperationen	NSA-Dokumente/The Intercept · EU-Parlamentsbericht STOA 2001 · Snowden/The Guardian Jun 2013 · Der Spiegel 2013 · WikiLeaks 2015 · ECCHR · OVG Münster 2019 · BVerfG 2025 · Bundesinnenministerium 2013

✓ VERIFIZIERTE QUELLENANGABEN

- [1] Landtag BW, Drucksache 17/9329 (August 2025): parlamentarische Anfrage – Rechenzentrumsstandort, Sicherheitsüberprüfung, kein unbeaufsichtigter Zugang (Regierungsposition)
- [2] §57a PolG BW (12. November 2025): Experimentierklausel – personenbezogene Polizeidaten an Privatunternehmen für KI-Training übermittelbar; rechtlich offener Kanal — landesrecht-bw.de
- [3] heise.de, 12. November 2025: Fehlen einer unabhängigen Prüfung bestätigt; Palantir-CIRT kontrolliert sich über eigenes CIRT selbst — heise.de
- [4] Brennan Center for Justice, FISA 702 Ressourcenseite 2026: NSA-Zwangsbefugnis; NSL-Schweigegebotsmechanismus – Deutschland hat keine Jurisdiktion — brennancenter.org
- [5] Sensors 2023, 23(6):3215, MDPI: 30+ Air-Gap-Covert-Channel-Angriffsmethoden überprüft; initialer Angriffsvektor in allen Fällen = USB/Supply-Chain/Insider (DOI: 10.3390/s23063215) — mdpi.com/1424-8220/23/6/3215
- [6] Guri, M.: RAMBO (arXiv:2409.02292, 2024) und PIXHELL (IEEE COMPSAC 2024) – EM- und akustische Covert Channels im Labor bestätigt; FDE-Wartungsbesuch = Stuxnet-artiger initialer Vektor
- [7] GFF – Gesellschaft für Freiheitsrechte: Verfassungsbeschwerden gegen Palantir in Bayern (2025); BW-Einsatz unter Beobachtung; Parallelklage erwartet — freiheitsrechte.org
- [8] BW Staatsministerium 29. Juli 2025: Europa-VerA – genannte Partner Airbus D&S + Schwarz Digits; kein Vertrag, keine Spezifikation, kein Budget bekanntgegeben — stm.baden-wuerttemberg.de/de/startseite
- [9] Koalitionsvertrag Grün-Schwarz BW 2026: Verpflichtung zur europäischen Alternative bis 2030 – politische Handlungsaufforderung, kein Mittelansatz — stuttgart-zeitung.de
- [10] Beteiligungsportal BW (September 2025): amtliche Folgenabschätzung – Europa-VerA-Kosten nicht bezifferbar; nur Palantir-Betriebskosten etatisiert — beteiligungsportal.baden-wuerttemberg.de
- [11] Abgeordnetenwatch.de – Grünen-MdL Fadime Tuncer / MP Cem Özdemir: Ausstiegsziel 2030 im Koalitionsvertrag bestätigt; kein Start der Alternativentwicklung bis Jul 2026 — abgeordnetenwatch.de
- [12] fragenstaat.de: IFG-Anträge auf den Palantir-Vertragstext – vom BW-Innenministerium als VS-NfD eingestuft abgelehnt — fragenstaat.de
- [13] DSGVO Art. 5 Abs. 1 lit. b und GG Art. 2 Abs. 1 / Art. 1 Abs. 1: Zweckbindung und informationelle Selbstbestimmung – Betroffene, deren Daten zu Polizeizwecken verarbeitet werden, haben nicht in die Nutzung für kommerzielles KI-Training eingewilligt

Alle Quellen geprüft und verifiziert Juni/Juli 2026. Primärquellen haben durchgehend Vorrang. Wo Sekundärberichte zitiert werden, sind sie auf namentlich genannte Journalisten in identifizierten Publikationen zurückzuführen.