VaultLM

VaultLM Sicherheitsübersicht

Datenfluss und Sicherheitsprinzipien für vertrauliche Dokument-KI

WAS VAULTLM IST

Ein kontrollierter Arbeitsbereich zwischen vertraulichen Dokumenten und KI. VaultLM wendet Rechte, Maskierung und Pseudonymisierung vor externer KI-Verarbeitung an und liefert Antworten mit Quellen und Audit Trail.

1. Dokumente

Originale gelangen in einen kontrollierten Vault mit Rechten und Aufbewahrung.

›

2. Schützen

Sensible Identifikatoren werden maskiert und pseudonymisiert.

›

3. Minimieren

Nur relevante und erlaubte Auszüge werden ausgewählt.

›

4. KI-Dienst

Der gewählte externe Dienst erhält minimalen geschützten Kontext.

›

5. Nachweis

Die Antwort kommt mit Quellenpassagen und protokollierter Nutzung zurück.

BLEIBT IN VAULTLM

Originaldateien, Identitätszuordnungen, Rechte und Aufbewahrung.

ZUR KI-VERARBEITUNG

Nur minimale, erlaubte und pseudonymisierte Auszüge.

SICHERHEITSPRINZIPIEN

Rechtegebunden

KI-Zugriff geht nie über das Recht hinaus, die Quelle zu öffnen.

Fail-closed

Ist erforderliche Maskierung nicht verfügbar, stoppt die externe Anfrage.

Dokumentgebunden

Externe Anfragen sind an erlaubte Vault-Quellen gebunden.

Prüfbar

Quellen, Dienstinformationen und Audit-Ereignisse unterstützen die Prüfung.

EHRLICHE GRENZEN

Reversible Maskierung ist Pseudonymisierung, nicht Anonymisierung. Automatische Erkennung ist nicht unfehlbar; menschliche Prüfung bleibt notwendig. VaultLM unterstützt Governance und Nachweise, garantiert aber nicht automatisch rechtliche Compliance.

AI-ACT-ZEITPLAN

Ab 2. August 2026 gelten weitere Bestimmungen des AI Act. Für Hochrisikosysteme gelten spätere Fristen: 2. Dezember 2027 für eigenständige Systeme und 2. August 2028 für Systeme, die in regulierte Produkte eingebettet sind.