TÜVIT

Inspired by Knowledge

AI Privacy Check

Gewährleistung des Datenschutzes für KI-basierte Anwendungen

Mit der zunehmenden Verbreitung von Künstlicher Intelligenz (KI) im digitalen Bereich entstehen neue Datenschutzrisiken, die standardisierte oder interne Datenschutzprüfungen möglicherweise nicht vollständig erfassen. Diese KI-spezifischen Risiken betreffen u. a. die unbeabsichtigte Offenlegung personenbezogener Daten durch KI-Modelle oder die Herausforderung, Daten dauerhaft zu löschen („Recht auf Vergessenwerden“).

Unser AI Privacy Check erweitert die traditionelle DSGVO-Bewertung um die spezifischen Datenschutzbedenken von KI. Dabei werden zwei Hauptaspekte betrachtet:

Risikobewertung zur Datenrekonstruktion: Wir führen eine technische Bewertung durch, um das Potenzial der Rekonstruktion von sensiblen (personenbezogenen) Daten aus Ihren KI-Modellen zu bestimmen. Dies umfasst eine gründliche Analyse der Architektur des Modells, der Trainingsprozesse sowie die Anwendung modernster Datenrekonstruktionstechniken.

Prüfung der Datenlöschung: Ergänzend beurteilen wir, ob Ihre KI-Systeme dem Prinzip des „Rechts auf Vergessenwerden“ folgen. Dieser Aspekt stellt sicher, dass Mechanismen vorhanden sind, um sensible Daten in Übereinstimmung mit den Anforderungen der DSGVO auf Anfrage aus Ihren Modellen „zu löschen“.

Indem Sie sich für unseren AI Privacy Check entscheiden, demonstrieren Sie Ihr Engagement für den Datenschutz, stärken gleichzeitig das Vertrauen bei Kund:innen und gewährleisten die Einhaltung von Vorschriften im dynamischen Bereich der KI-Technologie.

Ihr Vorteil: Unser Service ermöglicht es Ihnen, sich sicher in der Datenschutzlandschaft mit KI zu bewegen, indem er gewährleistet, dass Ihre Anwendungen die datenschutzrechtlichen Kriterien erfüllen und gleichzeitig sensible Daten vor Bedrohungen schützen. Dadurch stärken Sie das Vertrauen Ihrer Kund:innen und profitieren von Wettbewerbsvorteilen.

Seien Sie vorbereitet ...

Unsere Leistungen im Überblick

- Definition von Anforderungen („Fällt meine KI-Anwendung unter Datenschutzgesetze?“)
- Risikobewertung („Welche Auswirkungen haben KI-bezogene Datenschutzbedrohungen?“)
- Nachweis, ob eine Rekonstruktion sensibler (personenbezogener) Daten aus Ihren KI-Modellen möglich ist
- Bewertung und Nachweis, ob sensible Daten von Ihren KI-Modellen gelöscht/„vergessen“ werden können
- Unterstützung während des gesamten Entwicklungsprozesses
- Durchführung von Workshops und Schulungen
- Prüfung durch eine vertrauenswürdige und unabhängige Instanz

Unser Bewertungskonzept deckt alle KI-spezifischen Datenschutzthemen und entsprechenden Aspekte ab

- **KI und Datenschutz**
- **Computer Vision**
- **Risikobewertung von KI**
- **KI-Regulierung**
- **DSGVO**
- **Datenextraktion**
- **IP-Schutz**
- **Risiken und Schwachstellen von KI**
- **„Recht auf Vergessenwerden“**
- **Sensibilisierung von Mitarbeitenden**
- **Generative KI und Datenschutz**
- **AI Life-Cycle Management**

Über uns: Die TÜV Informationstechnik GmbH (TÜVIT), ein Unternehmen der TÜV NORD GROUP mit Geschäftsaktivitäten in weltweit 100 Ländern, ist einer der führenden Prüfdienstleister für IT-Sicherheit. Das Unternehmensportfolio deckt Themen wie Cyber Security, Evaluierung von Software und Hardware, Industrie 4.0, Datenschutz, ISMS, Smart Energy, Automotive Security, Mobile Security, eID und Vertrauensdienste sowie die Prüfung und Zertifizierung von Rechenzentren hinsichtlich ihrer physischen Sicherheit und Hochverfügbarkeit ab.

Kontakt: Vasilios Danos | Tel.: +49 201 8999-560 | v.danos@tuvit.de
TÜV Informationstechnik GmbH | Am TÜV 1 | 45307 Essen | tuvit.de