PRESSEMITTEILUNG

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 17. Oktober 2025

Datenschutzkonferenz veröffentlicht Orientierungshilfe zu KI-Systemen mit Retrieval Augmented Generation (RAG)

Die Konferenz der unabhängigen Datenschutzbehörden von Bund und Ländern (DSK) hat eine Orientierungshilfe für Unternehmen und Behörden veröffentlicht, die KI-Systeme mit sogenannter Retrieval Augmented Generation (RAG) bereits einsetzen oder einsetzen möchten. Auf 18 Seiten bietet die Orientierungshilfe rechtliche und technische Hinweise, wie die Potenziale solcher KI-Systeme genutzt und zugleich die Risiken für die Betroffenen verringert werden können.

RAG ist eine KI-Technologie, bei der große Sprachmodelle durch gezielten Zugriff auf unternehmens- oder behördeneigene Wissensquellen ergänzt werden, um kontextspezifische Antworten zu liefern. Typische Anwendungsbeispiele sind unternehmensinterne Chatbots, die auf aktuelle Geschäftsdaten zugreifen und wissenschaftliche Assistenzsysteme, die Forschungsdatenbanken nutzen. RAG-Systeme sollen die Genauigkeit, Nachvollziehbarkeit und Verlässlichkeit der KI-Ausgaben erhöhen, während die für große Sprachmodelle typischen Halluzinationen und unrichtigen Ausgaben vermindert werden sollen.

Meike Kamp, Berliner Beauftragte für Datenschutz und Informationsfreiheit und 2025 DSK-Vorsitzende: „RAG-Systeme können Unternehmen und Behörden dabei unterstützen, die Vorteile moderner KI zu nutzen und zugleich die damit einhergehenden Risiken für die Rechte und Freiheiten von betroffenen Personen zu vermindern. Entscheidend ist jedoch, dass ihr Einsatz von Anfang an datenschutzkonform gestaltet wird. Verantwortliche müssen Transparenz, Zweckbindung und die Wahrung der Betroffenenrechte jederzeit gewährleisten.“

RAG-Systeme können eigenständig entwickelt, betrieben und kontrolliert werden und damit Datenschutz-by-Design abbilden. Zudem können sie den Einsatz kleinerer und auch lokal betriebener Modelle ermöglichen, was beispielsweise einen Betrieb des Systems ohne Übermittlung personenbezogener Daten an Dritte wie etwa Hyperscaler ermöglicht. Damit kann die RAG-Methode einen wichtigen Beitrag zur digitalen Souveränität leisten.

RAG-Systeme bringen gleichwohl auch datenschutzrechtliche Risiken mit sich, die Verantwortliche im Blick haben müssen. Sie beseitigen beispielsweise nicht die datenschutzrechtlichen Probleme eines rechtswidrig trainierten Large Language Modells (LLMs). Je nach Ausgestaltung können sie aber Teil einer Antwort auf solche unrechtmäßig trainierten Systeme sein. Auch bleibt es herausfordernd, Transparenz, Zweckbindung und die Umsetzung von Betroffenenrechten im gesamten System sicherzustellen. Verantwortliche Stellen, die solche RAG-Systeme einsetzen wollen, müssen die datenschutzrechtlichen Bewertungen der einzelnen Verarbeitungen im Einzelfall vornehmen und ihre technisch-organisatorischen Maßnahmen immer auf dem aktuellen Stand halten.

Die neue Orientierungshilfe ist die dritte Veröffentlichung der DSK zu KI-Systemen seit 2024. Bereits erschienen sind Orientierungshilfen zum Einsatz sowie zur Entwicklung von KI-Systemen.

Mehr Informationen

- Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode
- Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen
- Orientierungshilfe zu Künstlicher Intelligenz und Datenschutz

Über die Datenschutzkonferenz:

Die Datenschutzkonferenz besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder. Sie hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Dies geschieht namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen.

Presse-Kontakt:

Vorsitz der Datenschutzkonferenz 2025
Berliner Beauftragte für Datenschutz und Informationsfreiheit
Telefon: +49 30 13889-900
E-Mail: presse@datenschutz-berlin.de
https://datenschutz-berlin.de/dsk2025
https://www.datenschutzkonferenz-online.de