Datenschutzkonferenz

# Orientierungshilfen zum KI-Einsatz

**[22.10.2025] KI-Systeme mit Retrieval Augmented Generation erhöhen die Genauigkeit und Zuverlässigkeit generativer Sprachmodelle. Auch Behörden können davon profitieren. Die Datenschutzkonferenz hat nun eine Orientierungshilfe zum rechtskonformen Einsatz veröffentlicht.**

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) einsetzen oder einsetzen möchten. Retrieval Augmented Generation verbindet generative KI in Form großer Sprachmodelle mit unternehmens- oder behördeneigenen Wissensquellen. So kann die KI Antworten liefern, die nicht allein auf Trainingsdaten basieren, sondern darüber hinausgehende Informationen einschließen. RAG-Systeme können die Genauigkeit und Verlässlichkeit der KI-Ausgaben erhöhen, während bekannte Schwächen wie Halluzinationen und unrichtige Ausgaben verringert werden. Typische Anwendungsbeispiele sind organisationseigene Chatbots, die auf aktuelle Geschäftsdaten zugreifen oder wissenschaftliche Assistenzsysteme, die Forschungsdatenbanken nutzen. Auch im Einsatz bei öffentlichen Behörden bietet RAG Vorteile, etwa durch kontextgenaue Assistenz bei der Navigation durch Prozesse und Informationen oder im Bürgerservice.

## Datenschutz by Design

Die DSK-Orientierungshilfe liefert auf 18 Seiten rechtliche und technische Hinweise, wie die Potenziale solcher KI-Systeme sicher genutzt werden können. RAG-Systeme können eigenständig entwickelt, betrieben und kontrolliert werden und damit „Datenschutz by Design“ abbilden. Zudem erlauben sie den Einsatz kleinerer, lokal betriebener Modelle, was den Betrieb ohne Übermittlung personenbezogener Daten an Hyperscaler ermöglicht. So kann die RAG-Methode auch einen wichtigen Beitrag zur digitalen Souveränität leisten.

## Herausforderungen bleiben

Trotz ihrer Vorteile bringen RAG-Systeme auch Risiken mit sich. So weist die DSK darauf hin, dass die datenschutzrechtlichen Probleme eines rechtswidrig trainierten LLMs nicht behoben werden. Auch bleibe es herausfordernd, Transparenz, Zweckbindung und die Umsetzung von Betroffenenrechten im gesamten System sicherzustellen. Verantwortliche Stellen, die RAG-Systeme einsetzen wollen, müssten die datenschutzrechtlichen Bewertungen der einzelnen Verarbeitungen im Einzelfall vornehmen, so die DSK, und ihre technisch-organisatorischen Maßnahmen auf dem aktuellen Stand halten. Die neue Orientierungshilfe ist die dritte Veröffentlichung der DSK zu KI-Systemen seit 2024.

(sib)

• 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

Stichwörter: Künstliche Intelligenz, Datenschutz, Datenschutzkonferenz