BfDI

# Praktisches Wissen über KI-Modelle gesucht

**[23.07.2025] Noch immer sind zahlreiche Fragen nach dem Schutz personenbezogener Daten beim Training von KI-Modellen offen. Um praktikable datenschutzrechtliche Ansätze zu entwickeln, hat die BfDI nun eine Konsultation gestartet. Gefragt sind Erfahrungen, Herausforderungen und Lösungen aus der Praxis.**

KI-Modelle, insbesondere große Sprachmodelle (Large Language Models, kurz: LLMs) müssen erst mit großen Datenmengen trainiert werden, um einsatzfähig zu werden. Sie können unter Umständen auch personenbezogene Informationen wortgetreu und sinngemäß aus ihren jeweiligen Trainingsdaten wiedergeben. Dementsprechend ist es möglich, dass Ergebnisse aus KI-Systemen Rückschlüsse auf bestimmte Personen zulassen – ein erhebliches Datenschutzrisiko. So hat beispielsweise der Europäische Datenschutzausschuss (EDSA) in einer Stellungnahme festgehalten, dass KI-Modelle personenbezogene Daten enthalten können, wenn sie mit solchen Daten trainiert wurden. Dieses Problem beschäftigt aber nicht nur die EU, sondern Aufsichtsbehörden weltweit – spätestens seit der Veröffentlichung von ChatGPT und der damit einhergehenden massiven Verfügbarkeit von neuen KI-Angeboten für Verbraucherinnen und Verbraucher.

## Austausch für praktikablen Datenschutz

„KI-Modelle revolutionieren zahlreiche Branchen und stellen uns zugleich vor große Herausforderungen in Sachen Transparenz, Sicherheit und Datenschutz“, sagt die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Louisa Specht-Riemenschneider. Um die datenschutzrechtlichen Herausforderungen bei der Planung, dem Training und der Nutzung solcher großen Sprachmodelle systematisch zu adressieren, hat die BfDI nun ein öffentliches Konsultationsverfahren gestartet. In Anerkennung der technischen und rechtlichen Komplexität ist es deren Ziel, konkrete praktische Erfahrungen, technische Einschätzungen und normative Überlegungen von Akteurinnen aus verschiedenen Bereichen einzuholen. Die Ergebnisse der Konsultation sollen dann zur Entwicklung von datenschutzkonformen Ansätzen im Umgang mit memorisierten Daten beitragen. Die wesentlichen Ergebnisse sollen in einem Konsultationsbericht zusammengefasst werden.

Das Verfahren läuft bis zum 10. August 2025, Stellungnahmen können per E-Mail eingesandt werden (Konsultation2025@bfdi.bund.de). Auf der BfDI-Website finden sich weitergehende Informationen inklusive der Konsultationsfragen.

(sib)

Stichwörter: Künstliche Intelligenz, Datenschutz