

Handreichung der BfDI: KI-Systeme datenschutzkonform einsetzen

Beim Einsatz von KI-Systemen werden personenbezogene Daten verarbeitet. Für Unternehmen stellt sich die Frage, wie KI datenschutzkonform genutzt werden kann und was dafür zu beachten ist. Die Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) hat eine Handreichung zum datenschutzkonformen Einsatz von KI in der Bundesverwaltung veröffentlicht, die auch für Unternehmen hilfreiche Informationen enthält.

Die von der BfDI veröffentlichte [Handreichung](#) über den datenschutzkonformen Einsatz und Training von KI-Systemen ist unmittelbar an die öffentliche Verwaltung adressiert. Sie kann jedoch auch für Unternehmen als Richtschnur zum rechtssicheren Einsatz von KI dienen.

Datenschutzrechtliche Herausforderungen von KI

Große Sprachmodelle (Large Language Models, kurz: LLM) wie ChatGPT oder Gemini werden mit kuratierten Trainingsdaten trainiert, auf deren Basis das System lernt, wie es sich verhalten muss. Aufgrund dieser Trainingsdaten wird ein neuronales Netz gebildet, mit dem das Modell operiert.

Hierbei ergeben sich verschiedene datenschutzrechtliche Herausforderungen, die in der Handreichung Berücksichtigung finden.

- **Black-Box-Charakter:** Der Output eines LLM ist aufgrund der besonderen Architektur nicht ohne Weiteres nachvollziehbar. Problematisch erscheint dies insbesondere bei der Umsetzung von Betroffenenrechten (Auskunftsanspruch, Recht auf Löschung oder Berichtigung). Da die Informationen als statistische Muster oder Wahrscheinlichkeiten in das Modell eingewoben sind, ist es schwierig, diese zu identifizieren, zu ändern oder zu entfernen.

- **Halluzinationen:** Trainingsdaten, auf denen das KI-Modell beruht, können fehlerhafte Informationen enthalten. Daraus ergibt sich eine Herausforderung für den Grundsatz der Datenrichtigkeit, der in Art. 5 Abs. 1 lit. D DSGVO verankert ist.
- **Erinnerung (Memorisierung) personenbezogener Daten:** Das Training von KI-Modellen erfolgt oftmals (auch) mit personenbezogenen Daten. Diese können unabsichtlich, aber auch durch gezielte Attacken, im Output des Modells enthalten sein. Zudem besteht die Gefahr, dass aufgrund der Zusammenführung personenbezogener Daten Rückschlüsse auf sensible Daten (wie z.B. auf politische Haltung oder Gesundheitsdaten) gezogen werden können. Die Verarbeitung von sensiblen Daten ist nur in eng begrenzten Fällen zulässig.
- **Voreingenommenheit:** Daten, mit denen das LLM trainiert wird, können einen Bias bzw. eine Voreingenommenheit aufweisen. Dies könnte im Konflikt mit dem Grundsatz von Treu und Glauben stehen (Art. 5 Abs. 1 lit. a DSGVO).
- **KI-Bereitstellung:** Bei der Bereitstellung eines KI-Modells können mehrere Dienstleister beteiligt sein. Hier ergeben sich gegebenenfalls Fragen hinsichtlich der datenschutzrechtlichen Verantwortlichkeit oder der Auftragsverarbeitung.
- **Datenübermittlung in Drittländer:** LLMs werden häufig außerhalb der EU gehostet oder es erfolgen Zugriffe von Drittstaaten auf in der EU gehostete KI-Systeme mit Modellen von Anbietern aus diesen Drittstaaten. Dadurch entstehen Risiken u.a. von staatlichen Zugriffen auf die übermittelten oder gespeicherten Daten oder auch Erschwernisse bei der Durchsetzung von Betroffenenrechten, etwa Lösungsansprüchen nach der DSGVO.

Empfehlungen der Handreichung

Bei der Bewältigung dieser und weiterer Herausforderungen bietet die Handreichung des BfDI Orientierung zum rechtssicheren Einsatz von KI-Systemen.

Unter anderem wird empfohlen:

- Bei der Auswahl von Anbietern sollte berücksichtigt werden, ob diese europäische Rechenzentren nutzen.
- Dem Bias sollte durch anerkannte Methoden gezielt entgegengewirkt werden.
- Personenbezogene Daten sollten anonymisiert oder pseudonymisiert werden.
- Es sollten, wo möglich, kleinere Sprachmodelle verwendet werden, um das Risiko einer unabsichtlichen Memorisierung zu verringern.
- Es sollten regelmäßige Schwachstellenüberprüfungen durch simulierte Systemattaken durchgeführt werden.



**Für alle weiteren Fragen rund um das Datenschutzrecht
stehen Ihnen gerne zur Verfügung**



Dr. Kristina Schreiber
+49 221 65065-337
kristina.schreiber@loschelder.de



Dr. Simon Kohm
+49 221 65065-200
simon.kohm@loschelder.de



Dennis Pethke, LL.M.
+49 221 65065-337
dennis.pethke@loschelder.de



Rebecca Moßner
+49 221 65065-465
rebecca.mossner@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE

Partnerschaftsgesellschaft mbB

Konrad-Adenauer-Ufer 11

50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110

info@loschelder.de

www.loschelder.de