LANDTAG NORDRHEIN-WESTFALEN
18. Wahlperiode

Drucksache **18/13352**

01.04.2025

Antwort

der Landesregierung

auf die Kleine Anfrage 5209 vom 26. Februar 2025
der Abgeordneten Sven W. Tritschler und Carlo Clemens AfD
Drucksache 18/12992

Datenschutz und Datensicherheit bei Nutzung des chinesischen KI-Chatbots „DeepSeek“ durch Landesbedienstete

Vorbemerkung der Kleinen Anfrage

Der chinesische KI-Chatbot DeepSeek hat in jüngster Zeit für Aufsehen gesorgt, aber auch erhebliche datenschutzrechtliche Bedenken hervorgerufen. Deutsche Datenschutzbehörden, darunter der Bremer Landesbeauftragte für Datenschutz, Timo Utermark, und der rheinland-pfälzische Datenschutzbeauftragte Dieter Kugelmann, sehen erhebliche Gefahren bei der Nutzung dieser KI.[1]

Es bestehen keine datenschutzrechtlichen Vereinbarungen für die Übermittlung personenbezogener Daten nach China seitens der Europäischen Kommission.[2] Berichte über eine umfassende Datenerfassung, ein aufgedecktes Datenleck und die Speicherung sensibler Nutzerdaten auf Servern in China werfen Fragen nach der Sicherheit bei der Nutzung dieses KI-Chatbots auf.
Insbesondere die Erfassung von IP-Adressen, Chatverläufen, hochgeladenen Dateien und sogar Tastaturanschlagmustern sind kritisch zu betrachten.

Einem Bericht zufolge scheint es bei DeepSeek „an so ziemlich allem zu fehlen“, was den Datenschutz betrifft.[3] Es ist daher von Bedeutung, ob und unter welchen Bedingungen Landesbedienstete DeepSeek auf ihren Diensthandys oder Dienstrechnern nutzen dürfen.

Die italienische Datenschutzbehörde hat DeepSeek bereits gesperrt, da die von dem Unternehmen übermittelten Informationen als „völlig unzureichend“ erachtet wurden. Zudem gab es einen Cyberangriff auf DeepSeek, der die Erreichbarkeit des Dienstes beeinträchtigte.[4]

[1] https://www.butenunbinnen.de/nachrichten/deepseek-ki-chatbot-datenschutz-bremen-100.html
[2] https://www.tagesspiegel.de/politik/digitalisierung-ki/chinesische-ki-anwendung-deutsche-datenschutzer-nehmen-deepseek-ins-visier-13113970.html
[3] https://www.derstandard.de/story/3000000255321/italiens-datenschutzbehoerde-sperrt-deepseek
[4] https://www.telepolis.de/features/KI-Startup-DeepSeek-unter-Beschuss-Italien-sperrt-USA-hackt-10265645.html

Datum des Originals: 01.04.2025/Ausgegeben: 07.04.2025

Die Ministerin für Heimat, Kommunales, Bau und Digitalisierung hat die Kleine Anfrage 5209 mit Schreiben vom 1. April 2025 namens der Landesregierung im Einvernehmen mit dem Minister des Innern beantwortet.

1. Welche konkreten Risiken sieht die Landesregierung im Hinblick auf die Nutzung des KI-Chatbots DeepSeek durch Landesbedienstete auf Diensthandys und Dienstrechnern, insbesondere im Hinblick auf den Schutz personenbezogener Daten und die Einhaltung der DSGVO?

2. Inwieweit berücksichtigt die Landesregierung die Bedenken der Datenschutzbehörden bei der Nutzung von KI-Chatbots wie DeepSeek?

3. Welche Vorkehrungen trifft die Landesregierung, um sicherzustellen, dass die bei der Nutzung von KI-Chatbots wie DeepSeek verarbeiteten Daten nicht für Zwecke missbraucht werden, die den Interessen des Landes und seiner Bürger zuwiderlaufen?

Die Fragen 1 bis 3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet:

Der Einsatz frei verfügbarer KI-Chatbots erfolgt im Rahmen des geltenden Rechts, wie beispielsweise der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 vom 14. April 2016).

Vor dem Hintergrund der europäischen Verordnung (EU) 2024/1689 über Künstliche Intelligenz vom 13. Juni 2024 und der Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024 hat das Ministerium für Heimat, Kommunales, Bau und Digitalisierung des Landes Nordrhein-Westfalen diesbezüglich einen Handlungsleitfaden für den Einsatz von Künstlicher Intelligenz in den Kommunalverwaltungen im Land Nordrhein-Westfalen erarbeitet und im Digitalbeirat - als Gremium mit kommunalen Praktikerinnen und Praktikern - empfohlen.

Mit den Landesressorts dauert der Erarbeitungsprozess einer möglichst gleichlautenden Regelung an.

Der Handlungsleitfaden verhält sich nicht zu speziellen Modellen, so auch nicht zum im Januar 2025 vorgestellten Modell DeepSeek R1, erfasst diesen aber inhaltlich. Der Einsatz von KI-Technologien ist danach nur zugelassen, wenn der Datenschutz gewahrt wird und die in der Datenschutz-Grundverordnung festgeschriebenen Grundsätze der Verarbeitung personenbezogener Daten eingehalten werden. Insbesondere dürfen derzeit keine personenbezogenen Daten als Input für Cloud-basierte KI-Chatbots verwendet werden.

Der Einsatz eines KI-Chatbots wird in der Landesverwaltung Nordrhein-Westfalen zurzeit im Rahmen des Pilotprojekts „NRW.Genius“ mit dem Ziel getestet, Landesbediensteten perspektivisch einen datenschutzkonformen KI-Chatbot für dienstliche Zwecke zur Verfügung stellen zu können.

4. Welche konkreten Maßnahmen hat die Landesregierung ergriffen oder plant sie zu ergreifen, um die Nutzung von DeepSeek durch Landesbedienstete zu reglementieren und die Datensicherheit zu gewährleisten?

Es gelten die grundsätzlichen Anforderungen an die Nutzung von web-basierten Diensten und den sicheren Umgang mit dienstlichen Informationen. Die Landesregierung schafft mit „NRW.Genius“ ein eigenes, den jeweiligen dienstlichen Anforderungen entsprechendes KI-Werkzeug und zeigt mit dem derzeit in Entwicklung befindlichen Handlungsleitfaden den Weg zu einem sicheren Einsatz von KI auf.

5. Hat die Landesregierung Kenntnis darüber, ob DeepSeek eine europäische Niederlassung oder einen zuständigen gesetzlichen Vertreter hat?

Eine europäische Niederlassung oder ein zuständiger gesetzlicher Vertreter sind der Landesregierung nicht bekannt.