

GZ: D231.000
2025-0.252.008

Sachbearbeiter: Dr. Andreas ZAVADIL

Betrifft: Richtlinie zum Einsatz von Large Language Models (LLMs) in der Datenschutzbehörde

1. Allgemeines

Künstliche Intelligenz (KI) umfasst eine Vielzahl von Technologien, die zunehmend in Wirtschaft und Gesellschaft eingesetzt werden. Eine spezielle Form der KI sind Sprachmodelle, auch bekannt als **Large Language Models (LLMs)**. Bekannte Beispiele für auf LLMs basierende Chatbots und andere Anwendungen sind unter anderem **ChatGPT, Gemini und Meta AI**. Mittlerweile sind diese LLM-Anwendungen oft zu multimodalem Arbeiten fähig, können also etwa auch Bilder als Input oder Output verarbeiten. Diese LLM-Anwendungen können bei einigen Aufgaben durchaus hilfreich sein, es bestehen bei ihrer Nutzung allerdings auch Risiken.

Grundsätzlich sind Bedienstete der Datenschutzbehörde dazu verpflichtet, dienstliche Aufgaben ausschließlich mit den vom Dienstgeber bereitgestellten und genehmigten Mitteln zu erfüllen.

2. Einsatz von LLM-Anwendungen in der Datenschutzbehörde

Abweichend von Punkt 1 ist die Nutzung von LLM-Anwendungen zur Erfüllung dienstlicher Aufgaben zulässig, sofern sämtliche der folgenden Voraussetzungen vollständig erfüllt sind:

- a) **Keine Verarbeitung personenbezogener Daten:** Es dürfen keine personenbezogenen Daten, einschließlich Daten juristischer Personen, in LLM-Anwendungen eingegeben werden oder Dokumente, die personenbezogene Daten enthalten, hochgeladen werden.
- b) **Keine vertraulichen oder sensiblen Informationen:** Es dürfen keine Betriebs- oder Geschäftsgeheimnisse sowie keine Informationen von anderen öffentlichen Stellen oder sonstige schutzwürdige Daten eingegeben oder Dokumente, welche derartige Informationen beinhalten (können), hochgeladen werden.
- c) **Kein Ersatz für rechtliche oder sachliche Prüfungen:** Aktuell funktionieren die LLM-Anwendungen so, dass sie vereinfacht gesagt das jeweils nächstpassende Wort vorhersagen und darauf basierend einen Text erstellen. Möglich ist auch eine Echtzeitsuche im Internet. Das Modell hat daher jedoch kein „Wissen“. Aufgrund des Risikos von Fehlinformationen oder sog. Halluzinationen dürfen LLM-Anwendungen daher jedenfalls nicht zur Beurteilung oder Klärung von Rechts- oder Sachverhaltsfragen verwendet werden.

- d) **Keine Entscheidungsfindung durch LLM-Anwendungen:** LLM-Anwendungen dürfen daher auch nicht – auch nicht teilweise – für die Erstellung von Entscheidungsvorschlägen in Verfahren vor der Datenschutzbehörde herangezogen werden. Es wird ausdrücklich darauf hingewiesen, dass für die Datenschutzbehörde keine Rechtsgrundlage zur automatisierten Entscheidungsfindung gemäß Art. 22 Abs. 2 lit. b DSGVO besteht.
- e) **Einschränkung auf LLM-Anwendungen von bestimmten Betreibern:** Es dürfen nur LLM-Anwendungen von Betreibern genutzt werden, die ihren Sitz i) im EWR oder ii) in Drittstaaten haben, für die aktuell ein Angemessenheitsbeschluss gemäß Art. 45 DSGVO besteht. Daraus folgt, dass die gängigsten LLM-Anwendungen ChatGPT, Gemini, Meta AI und Mistral aktuell verwendet werden können. Aktuell nicht zulässig wäre daher die LLM-Anwendung DeepSeek.
- f) **Anzeigepflicht:** Die grundsätzliche Nutzung von LLM-Anwendungen im Rahmen dienstlicher Aufgaben ist der jeweiligen Abteilungsleitung vorab mitzuteilen. Es ist anzugeben, welches Produkt zu welchen Zwecken verwendet wird. Darüber hinaus sind Änderungen anzugeben.

Unter **Einhaltung all dieser Voraussetzungen können** LLMs z. B. für folgende Zwecke genutzt werden:

- Formulierungshilfen für allgemeine, nicht personenbezogene Texte (z. B. Bekanntmachungen für die DSB-Website, Prüfung von Leistungsaufträgen oder Textbausteinen hinsichtlich Verständlichkeit und Präzisierung)
- Sprachliche Überarbeitung von neutralen Texten (z. B. Verbesserung der Verständlichkeit oder stilistische Anpassung von Texten ohne vertrauliche Inhalte)
- Erstellung von Gliederungen oder Inhaltsvorschlägen für Präsentationen (z. B. für interne Schulungen oder Vorträge)
- Zusammenfassung öffentlicher Dokumente (z. B. EDSA-Leitlinien, um einen raschen Überblick zu erhalten)
- Brainstorming für Projektnamen, Slogans oder Kampagnenideen (z. B. im Rahmen von EU-geförderten Projekten)
- Allgemeine Unterstützung bei Übersetzungen (z. B. von nicht-vertraulichen Texten ins Englische)
- Technische Erklärungen oder Definitionen für interne Zwecke (z. B. „Was ist ein LLM?“ oder „Wie funktioniert Verschlüsselung?“)

Aufgrund des Risikos, personenbezogene Daten oder vertrauliche bzw. sensible Informationen zu übersehen, wird empfohlen, jeweils nur Sätze bzw. Absätze übersetzen zu lassen. Gleiches gilt für Zusammenfassungen, soweit dies im Hinblick auf den Gesamtzusammenhang möglich ist.

2. April 2025

Der Leiter der Datenschutzbehörde:

SCHMIDL