Der Bayerische Landesbeauftragte
für den Datenschutz

AI IN A NUTSHELL 3

Einsatz eines LLM-gestützten Chatbots

Ausgangslage | Einsatzszenario

Die Einsatzmöglichkeiten von LLM (Large Language Model)-gestützten Chatbots sind vielfältig: Sie können ergänzend sowohl für behördeninterne als auch für externe Kommunikation genutzt werden. Unter einem LLM-gestützten Chatbot wird im Folgenden ein KI-System auf Basis eines Großen Sprachmodells verstanden, das Antworten probabilistisch, das heißt auf Wahrscheinlichkeiten basierend, generiert. Hiervon zu unterscheiden sind rein regelbasierte Chatbots, deren Eingaben und Ausgaben vorab, beispielsweise durch feste Entscheidungsbäume, eng definiert und technisch leichter vorhersehbar sind.

Behördenintern kann ein Chatbot die Beschäftigten beispielsweise dabei unterstützen, für ihre Tätigkeit relevante Dokumente, Textpassagen oder Fundstellen im Intranet beziehungsweise im Dokumentenmanagementsystem zu finden. Als Mittel der externen Kommunikation sind LLM-gestützte Chatbots häufig auf Webseiten öffentlicher Stellen eingebunden; sie dienen dort beispielsweise der Erstbeantwortung von Bürgeranfragen auf der Grundlage der auf der Website veröffentlichen Informationen.

Zentrale KI-datenschutzrechtliche Fragestellungen zur Beachtung bei Beschaffung und Nutzung von LLM-gestützten Chatbots

Hinweis: Zum Datenschutz bei KI-Projekten bayerischer öffentlicher Stellen allgemein ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung, Orientierungshilfe, Stand 3/2026, im Internet abrufbar unter https://www.datenschutz-bayern.de/ki (OH KI). Zu den spezifischen Fragestellungen im Folgenden vergleiche Verweise.

[1] Beschaffung

Thematik: Im Zusammenhang mit der Beschaffung eines LLM-gestützten Chatbots durch eine bayerische öffentliche Stelle ergeben sich eine Vielzahl praktischer sowie rechtlicher Fragestellungen (vgl. allgemeine die Empfehlungen zu Planung und Beschaffung von KI-Systemen, OH KI, Rn. 370 f.). Dies erfordert im Vorfeld eine umfassende Prüfung des geplanten Einsatzes des Chatbots unter Klärung der technischen und rechtlichen Rahmenbedingungen für dessen Nutzung (vgl. hierzu allgemein Bayerischer Landesbeauftragter für den Datenschutz, Datenschutzkonzepte für Digitalisierungsvorhaben, Aktuelle Kurz-Information 64, Stand 9/2025, Internet: https://www.datenschutz-bayern.de/infothek). Allem voran steht dabei die Frage, ob und inwieweit eine Verarbeitung personenbezogener Daten bei der Nutzung des Chatbots überhaupt erforderlich ist.

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

Insbesondere erforderliches Tätigwerden:

- Im Rahmen dieser Vorab-Prüfung sind nicht nur die geplanten Nutzungsszenarien sorgfältig zu klären, sondern insbesondere auch folgende Fragestellungen: Soll ein offenes oder abgeschottetes System zum Einsatz kommen (vgl. OH KI, Rn. 146 f., 317), ein RAG-Subsystem angebunden werden (vgl. hierzu Bayerischer Landesbeauftragter für den Datenschutz, Anbindung eines RAG-Subsystems an ein KI-System mit Sprachmodell, AI in a Nutshell 1, Internet: https://www.datenschutz-bayern.de/ki, sowie OH KI, Rn. 178 ff.), ein bereits vortrainiertes KI-System beschafft werden (vgl. zur Entwicklung und zum Training von KI-Systemen OH KI, Rn. 148 ff.) und/oder ein cloudbasiertes Produkt genutzt werden soll (vgl. zum „Sonderfall: Cloud" OH KI, Rn. 363 f.)?
- Außerdem sollte besonderes Augenmerk auf die Prüfung und gegebenenfalls den Abschluss von Verträgen (wie beispielsweise Auftragsverarbeitungsvereinbarungen nach Art. 28 Abs. 3 DSGVO, vgl. zur Auftragsverarbeitung OH KI, Rn. 288 ff.) gelegt werden.

[2] Implementierung

Thematik: Enthält ein LLM-gestützter Chatbot bereits im Zeitpunkt der Bereitstellung durch den Anbieter zur Nutzung – je nach vorhergehendem Training – personenbezogene Daten, muss die einsetzende öffentliche Stelle im Rahmen der Implementierung des Chatbots insbesondere dessen datenschutzkonforme Verwendung sicherstellen und nachweisen (Art. 5 Abs. 2 DSGVO) (vgl. allgemein zur Bereitstellung und Implementierung von KI-Systemen OH KI, Rn. 166 ff.):

Insbesondere erforderliches Tätigwerden:

- Soweit ein extern vortrainierter Chatbot genutzt werden soll: Durchführung einer „angemessenen Bewertung" der Datenschutzkonformität des Chatbots sowie gegebenenfalls Ergreifen sogenannter risikomindernder Maßnahmen (vgl. OH KI, Rn. 169);
- Erstellung erforderlicher rechtlicher Dokumentationen wie Datenschutz-Folgenabschätzung (vgl. OH KI, Rn. 349 ff.) und Verzeichnis von Verarbeitungstätigkeiten (vgl. OH KI, Rn. 356 f.);
- Sicherstellung der Gewährleistung der Transparenzpflichten (vgl. OH KI, Rn. 296 ff.) sowie der Betroffenenrechte (vgl. OH KI, Rn. 310 ff.) gegenüber internen wie externen Nutzern;

  Hinweis: Nach Art. 50 Abs. 1 KI-Verordnung müssen Nutzende bei der Verwendung von KI-Systemen, die für die direkte Interaktion mit natürlichen Personen bestimmt sind, grundsätzlich darauf aufmerksam gemacht werden, dass sie mit einer Maschine interagieren. Dies ist vorliegend insbesondere gegenüber **externen Nutzern** von LLM-gestützten Chatbots zu beachten, damit sie eine informierte Entscheidung treffen können, mit der Nutzung fortzufahren oder den Prozess abzubrechen (vgl. OH KI, Rn. 56).

- Implementierung der relevanten technischen und organisatorischen Maßnahmen (vgl. allgemein OH KI, Rn. 343 ff.) sowie Konfiguration des Chatbots.

  Dies betrifft im Zusammenhang mit der Nutzung eines Chatbots insbesondere die Minimierung des Risikos etwaiger unzulässiger Eingaben personenbezogener Daten (vgl. OH KI, Rn. 347), die Deaktivierung des Nachtrainings des Chatbots mit den Eingabedaten (vgl. OH KI, Rn. 162 ff., 347) sowie die Deaktivierung der „Historie" (vgl. OH KI, Rn. 147, 347). **Bei behördeninterner Nutzung** sollte zusätzlich die Verarbeitung der Nutzerdaten durch Bereitstellung von Funktionsaccounts und/oder den Einsatz von Schnittstellen minimiert werden (vgl. OH KI, Rn. 173 f.).

- **Nur bei einer (auch) behördeninternen Nutzung:** Erstellung einer Dienstanweisung oder Abschluss einer Dienstvereinbarung mit Vorgaben dazu, ob, unter welchen Voraussetzungen und zu welchen konkreten Zwecken der Chatbot eingesetzt werden darf (vgl. OH KI, Rn. 374 ff.), sowie Schulung der Beschäftigten der öffentlichen Stelle zu Datenschutzrisiken im Zusammenhang mit dem Chatbot (vgl. OH KI, Rn. 77 ff., 347, 383 f.).

[3] Nutzung

Thematik: Der Einsatz eines LLM-gestützten Chatbots auf der Grundlage bestehender Verarbeitungsbefugnisse – und dabei also insbesondere auch im Rahmen des Erforderlichen (vgl. OH KI, Rn. 250) – entspricht aus datenschutzrechtlicher Sicht oftmals der Nutzung eines Betriebsmittels.

Insbesondere erforderliches Tätigwerden:

- Regelmäßige Überprüfung und bei Bedarf Anpassung der den Chatbot betreffenden Datenschutzmaßnahmen (vgl. OH KI, Rn. 117, 379);

- **Besonders bei behördeninterner Nutzung:** Erforderlichkeit der Prüfung der Ausgaben eines Chatbots insbesondere hinsichtlich ihrer Diskriminierungsfreiheit, Richtigkeit und Vollständigkeit sowie auf etwaigen Personenbezug beziehungsweise das Vorliegen einer Rechtsgrundlage für die entsprechende Datenverarbeitung (vgl. OH KI, Rn. 187 ff.).

Hinweis: Unabhängig von dem konkreten zur Anwendung kommenden Produkt und dem jeweiligen Einsatzszenario sind sämtliche Vorgaben des Datenschutzrechts und insbesondere der Datenschutz-Grundverordnung einzuhalten und nachzuweisen, sobald und soweit bayerische öffentliche Stellen personenbezogene Daten mittels Künstlicher Intelligenz verarbeiten (näher OH KI, Rn. 192 ff.).