

# Freie und Hansestadt Hamburg

Senatskanzlei

**Handlungsanweisung im Umgang mit LLMoin**  
Stand 25.07.2025

# Handlungsanweisungen für LLMoin

## Einleitung

LLMoin steht den Beschäftigten der FHH über die Single-Sign-On (SSO) Anmeldung zur Verfügung. Die Nutzung von LLMoin ist **freiwillig**. Im Rahmen der Unterstützung routinemäßiger Textaufgaben kann LLMoin die Effizienz der Verwaltung steigern und die Dienstleistungsqualität der Hamburger Verwaltung erhöhen.

Dieses Dokument beschreibt, wie der KI-Sprachassistent LLMoin der Senatskanzlei der FHH konkret eingesetzt werden darf. Die hier enthaltenen Vorgaben werden aufgrund der hohen Entwicklungsdynamik von Sprachmodellen regelmäßig **evaluiert**, ggfs. **angepasst** und mit Datum versehen. Anpassungen bzw. Erweiterungen werden ohne vorherige Ankündigung vorgenommen. Dieses Dokument sollte daher regelmäßig zur Kenntnis genommen werden.

## 1. Welche Funktionen hat LLMoin?

LLMoin bietet die nachfolgenden Funktionen:

- Zusammenfassung:

Lange Texte und Dokumente werden zusammengefasst. Mögliche Optionen bei der Zusammenfassung sind Länge, Sprachstil und Textart. LLMoin analysiert bspw. große Mengen an Feedback und erstellt Zusammenfassungen, die überprüft und weiterverarbeitet werden können.

- Inhaltsgenerierung:

Aus Stichpunkten und anderen Vorgaben wird ein Text generiert. Mögliche Einstellungsoptionen sind: Länge, Sprachstil, Anrede, Textart und Format. LLMoin erstellt bspw. Entwürfe für Vermerke aus unstrukturierten Daten, die von den Nutzer:innen weiterverarbeitet werden, oder gibt Feedback zu Rechtschreibung und Grammatik eines schon existierenden Dokuments oder schreibt den Inhalt in eine bürgernahe Sprache um. LLMoin erstellt bspw. erste Antwortvorschläge und findet relevante Informationen für Bürgeranfragen, die von den Nutzer:innen weiter überprüft und angepasst werden.

- Recherche:

Nutzer:innen können Fragen an vorher definierte Datensätze oder ad-hoc bereitgestellte Dokumente stellen. Diese werden durch das Modell in natürlicher Sprache und mit Verweis auf das relevante Dokument beantwortet.

- Freies Prompten<sup>1</sup>:

Im Gegensatz zu den geführten Prompts der ersten drei Funktionen erlaubt das „freie Prompten“, frei und flexibel Eingaben zu formulieren, um maßgeschneiderte Antworten zu erhalten. Diese Funktion ist vor allem für erfahrene Nutzer:innen gedacht, die durch ihre Erfahrung im Umgang mit LLMs oder durch das Absolvieren der LLMoin Schulungsunterlagen (insb. Modul 4) erlernt haben, wie sie Eingaben formulieren müssen, um die gewünschten Antworten zu erhalten.

## 2. Was muss ich vor der Nutzung von LLMoin erledigt haben?

Eine effiziente und korrekte Verwendung von LLMoin kann nur durch **kompetente** und kritische Nutzer:innen erreicht werden. Daher besteht neben der Einhaltung der nachstehenden Bedingungen auch die **Pflicht**, sich mit der Funktionsweise von LLMs (Sprachmodellen), insbesondere deren Stärken und Schwächen sowie den technischen Rahmenbedingungen von LLMoin auseinanderzusetzen. Konkret bedeutet dies, dass alle LLMoin Nutzer:innen über Grundlagen von

---

<sup>1</sup> „Prompten“ oder auch „Prompting“ bezeichnet das Eingeben von Anfragen oder Befehlen, um passende Antworten oder Aktionen von einem KI-Modell, wie LLMoin, zu erhalten.

LLMs und Limitationen, wie Halluzinationen und Biases, Grundkenntnisse besitzen müssen. Des Weiteren müssen Nutzer:innen sich mit den Themen Hochrisiko-Bereich und erlaubte Anwendungen in diesen Bereichen auseinandersetzen. Für beide Themenkomplexe bieten wir umfassende LLMoin-**Schulungsunterlagen**<sup>2</sup> an, in denen diese Kompetenzen – insbesondere in Modul 1 und Modul 3 - aufgebaut werden. Darüber hinaus wird in den Schulungsunterlagen detailliertes Spezialwissen zu LLMoin und zum sogenannten Prompten vermittelt.

### 3. Wofür und wie darf LLMoin verwendet werden? Wofür und wie nicht?

LLMoin ist grundsätzlich für alle textbasierten Aufgaben im **dienstlichen Kontext** nutzbar.

Die Nutzung von LLMoin zu **privaten Zwecken** darf nur gelegentlich erfolgen. Dienstlich Belange dürfen hierbei nicht beeinträchtigt werden. Eine Nutzung zu erwerbswirtschaftlichen Zwecken außerhalb eines dienstlichen Kontextes ist nicht gestattet. Die unabgestimmte Nutzung der LLMoin-API zur Integration in andere Produkte oder eine exzessive<sup>3</sup> Nutzung ist untersagt.

LLMoin ist **nicht** für die Bearbeitung von **Verschlusssachen** freigegeben.

Auch **untersagt** sind **unethische Interaktionen** mit LLMoin. Darunter fallen bspw. Erstellung von Hassrede, Diskriminierung, Belästigungen, irreführenden oder sonstigen böswilligen Inhalten, Nutzung zur Unterstützung illegaler Aktivitäten, Ausnutzung von Schwächen oder Sicherheitslücken von LLMoin oder im dahinterliegenden System und Verwendung zur gezielten Manipulation von Prozessen oder Menschen.

Darüber hinaus ist die Nutzung von LLMoin für das sog. **Profiling** oder für eine **soziale Bewertung** von Personen **untersagt**. Dies meint eine Verarbeitung personenbezogener Daten durch KI-Systeme, um bestimmte Aspekte einer natürlichen Person zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, soziales Verhalten, Aufenthaltsort oder Bewegungen zu analysieren oder vorherzusagen. Des Weiteren ist auch die Nutzung von LLMoin zum Zwecke der **Strafverfolgung** oder **Gefahrenabwehr untersagt**.

Die Verwendung von Antworten aus LLMoin kann im Hochrisiko-Bereich gemäß Anhang III der KIVO oder im Nicht-Hochrisiko-Bereich liegen. In Hochrisiko-Bereichen gemäß Anhang III der KIVO besteht ein erhöhtes Risiko für die Gesundheit, Sicherheit oder Grundrechte von Personen. Eine Nutzung von LLMoin im **Hochrisiko-Bereich** ist unzulässig. In Bereichen gemäß Anhang III der KIVO dürfen Antworten aus LLMoin nur in einem Rahmen genutzt werden, bei dem das Ergebnis einer Sachentscheidung (z.B. im Rahmen eines Verwaltungsverfahrens) **nicht wesentlich** beeinflusst wird. Nur dann ist LLMoin nicht als Hochrisiko-Anwendung nach Art. 6 Abs. 3 KIVO einzustufen. Die Abgrenzung zum Hochrisiko-Bereich wird in den Schulungsunterlagen und im Anhang zu dieser Handlungsanweisung ausführlich beschrieben. Weitere Einzelheiten dazu, was es heißt, dass LLMoin eine Sachentscheidung wesentlich beeinflusst, sind im **Anhang zu Hochrisiko-Anwendungen** aufgeführt.

**Untersagt** ist schließlich die Verwendung von (technischen) Mitteln und Werkzeugen, um **personenbezogene Daten** aus der **Wissensbasis des KI-Modells** von LLMoin zu **extrahieren**. Gleiches gilt für die Nutzung von LLMoin selbst zu dem Zweck, personenbezogene Daten aus der Wissensbasis des KI-Modells **abzufragen**. Ausgenommen sind Abfragen, die sich auf Daten beziehen, die von den dahinter stehenden Personen mit sehr hoher Wahrscheinlichkeit bereits **selbst öffentlich zugänglich gemacht** wurden, als sie zur Entwicklung des KI-Modells von LLMoin genutzt worden sind (z.B. der Vor- und Nachname der letzten Ersten Bürgermeister der Freien und

<sup>2</sup> Die Schulungsunterlagen sind als E-Learning Lernpfad auf der ZAF-Plattform vorzufinden.

<sup>3</sup> Untersagt ist hiermit jede Handlung, die geeignet ist, den ordnungsgemäßen Betrieb der Anwendung zu beeinträchtigen, insbesondere die IT-Systeme übermäßig zu belasten.

Hansestadt Hamburg). Mit Wissensbasis gemeint sind die Daten, mit denen das KI-Modell zur Nutzung entwickelt („trainiert“) worden ist. **Nicht** gemeint sind die Daten, die Teil des Prompts / der Eingabe und ggfs. hochgeladen worden sind. Für diese gelten die Beschränkungen unter Ziffer 4.

#### 4. Welche Beschränkungen gelten für Eingaben/Prompts in LLMoin?

Behördeninterne Daten und Dokumente sowie Dokumente, die Unternehmensdaten enthalten, **dürfen** grundsätzlich als Teil der Eingabe / des Prompts in LLMoin hochgeladen werden.

Die Eingabe von Daten Minderjähriger, Daten nach Art. 9 DSGVO<sup>4</sup> und Art. 10 DSGVO<sup>5</sup>, Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, sowie Personalaktendaten, soweit sie vertrauliche oder höchstpersönliche Daten darstellen, ist **untersagt**. Sozialdaten sind Einzelheiten aus einem Sozialversicherungsverhältnis, wie unter anderem Versicherungsnummer, Versicherungsart, -leistungen und -dauer. Daten, die dem Berufsgeheimnis unterliegen, sind insbesondere Einzelheiten aus der Beziehung zu Angehörigen freier Berufe (z.B. Ärzte, Rechtsanwälte, Apotheker, Steuerberater, Wirtschaftsprüfer). Als besonderes Amtsgeheimnis sind das Sozial-, Steuer-, Statistik- und Wahlgeheimnis anzusehen. Es ist sicherzustellen, dass alle Dokumente und Eingaben frei von solchen Daten sind.

Schließlich sind die nachfolgenden Eingaben **untersagt**: Eingabe großer Datensammlungen, die nicht allein zur Wahrnehmung eigener Aufgaben beim Betroffenen erhoben wurden (z.B. zur Entscheidung über einen Antrag einer Bürgerin), sondern aus unterschiedlichen Quellen zusammengeführt wurden, um entweder Zusammenhänge zwischen den Daten zu hiervon abweichenden neuen Zwecken zu erkennen (z.B. Big Data-Analysen zur Entwicklung eines KI-Systems oder umfangreiche Zusammenführung von Nutzungsdaten von mehreren Websites zur Abwehr missbräuchlicher Websitenutzung), oder, um eine Grundlage für eine Entscheidung gegenüber einem Beschäftigten oder Bürger zu schaffen; Eingabe von Daten aus Personenstands- und Melderegister oder Meldedaten mit Sperrvermerken gemäß § 51 Abs. 1 und 5 Bundesmeldegesetz oder Personenstandsdaten gemäß § 63 Personenstandsgesetz; Eingabe umfangreicher Daten im Rahmen der amtlichen Statistik für die Übermittlung an Dritte.

#### 5. Welche Beschränkungen gelten für Verwendungen von Antworten aus LLMoin?

Aufgrund der weitreichenden Nutzungsmöglichkeiten ist ein verantwortungsvoller Umgang mit den Antworten aus LLMoin durch die Nutzer:innen geboten. Bei LLMoin handelt es sich um eine innovative Technologie, deren Einsatz wohlüberlegt zu erfolgen hat. Die **ungeprüfte Verwendung** von Antworten ist **untersagt**. Vor einer Veröffentlichung müssen die Antworten auf geheime oder geschützte Inhalte geprüft werden.

**LLMoin darf keine Entscheidungen anstelle eines Menschen treffen und den Menschen nicht von seiner Verantwortlichkeit als Entscheidungsträger entbinden. Außerdem müssen die generierten Ergebnisse stets auf sprachliche und inhaltliche Richtigkeit sowie Angemessenheit und Aktualität überprüft und bei Bedarf angepasst werden.**

<sup>4</sup> Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

<sup>5</sup> Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen.

## 6. Welche Folgen haben Verstöße gegen die Handlungsanweisungen?

Für eine Nutzung von LLMoin, die entgegen diesen Handlungsanweisungen erfolgt, ist die Senatskanzlei der FHH **nicht verantwortlich**. Für Antworten auf Grundlage verbotener Eingaben nach Ziffer 4, für die verbotene Verwendung von Antworten nach Ziffer 5 sowie für die unzulässige Nutzung von LLMoin nach Ziffer 3 ist die Senatskanzlei der FHH datenschutzrechtlich nicht verantwortlich.

Soweit LLMoin entgegen den Handlungsanweisungen als Hochrisiko-Anwendung genutzt wird, kann dies eine **eigene Verantwortlichkeit** nach Art. 25 Abs. 1 Buchstabe c KIVO zur Folge haben und Anbieterpflichten für Hochrisiko-KI-Systeme nach sich ziehen, wie u.a. Durchführung von Konformitätsbewertungsverfahren, technische Dokumentationspflichten und Qualitätsmanagement.

## 7. Was ist bei fragwürdigen Antworten zu tun?

Sollten Ergebnisse von LLMoin als fragwürdig unter den oben genannten Aspekten erscheinen, sind Nutzer:innen aufgefordert, diese Sachverhalte an die fachliche Leitstelle (llmoin@sk.hamburg.de) zu melden.

### Lokale Handlungsanweisungen

Je nach Behörde und Fachbereich gibt es – neben diesen Handlungsanweisungen der Senatskanzlei der FHH – ggfs. weitere „lokale“ Anweisungen zur Nutzung von LLMoin. Dies gilt insbesondere in den in Anhang III der KI-Verordnung genannten Hoch-Risiko Bereichen. Diese werden gesondert erteilt.

**Bitte lies diesen Anhang aufmerksam, insbesondere, wenn du in einem Hoch-Risiko Bereich arbeitest.**

## Anhang zu Hochrisiko-Anwendungen

LLMoin darf nicht als Hochrisiko-Anwendung im Sinne der KI-Verordnung genutzt werden. Um dies zu gewährleisten, muss verhindert werden, dass ein erhebliches Risiko der Beeinträchtigung in Bezug auf Gesundheit, Sicherheit oder Grundrechte natürlicher Personen besteht. Dies ist der Fall, wenn LLMoin das Ergebnis der Entscheidungsfindung nicht wesentlich beeinflusst. Was heißt das genau?

### 1. Welche Nutzungen gelten als Hochrisiko-Anwendungsbereich?

Der Anwendungsbereich für Hochrisiko-Anwendungen ergibt sich aus [Art. 6](#) der KI-Verordnung i.V.m. [Anhang III](#). Bei einer Nutzung von LLMoin in der Verwaltung sind insbesondere folgende Bereiche als mögliche Hochrisiko-Anwendungen genauer zu betrachten:

- Kritische Infrastruktur: Wasser-, Gas-, Wärme-, Stromversorgung
- Bildung: insbesondere Zugang, Bewertung oder Überwachung
- Personal: insbesondere Einstellung, Beförderung, Kündigung oder Zuweisung von Aufgaben
- Zugänglichkeit und Inanspruchnahme öffentlicher Leistungen und Dienste: insbesondere soziale Leistungen
- Strafverfolgung
- Migration, Asyl und Grenzkontrolle
- Rechtspflege und demokratische Prozesse

**Ungeachtet davon gilt ein KI-System immer dann als hochriskant, wenn es ein Profiling natürlicher Personen vornimmt, daher ist diese Nutzung in Ziffer 3 der Handlungsanweisung ausgeschlossen.**

### 2. Wie verhalte ich mich in einem Hochrisiko-Anwendungsbereich?

In den in [Anhang III](#) genannten Hochrisiko-Bereichen gilt LLMoin nur dann **nicht** als Hochrisiko-Anwendungen (*und darf somit genutzt werden*), wenn **kein erhebliches Risiko** der Beeinträchtigung in **Bezug auf die Gesundheit, Sicherheit oder Grundrechte** natürlicher Personen besteht. Dies ist unter anderem der Fall, wenn das **Ergebnis der Entscheidungsfindung nicht wesentlich beeinflusst wird**. Erlaubte Anwendungsbereiche, wo es keine wesentliche Beeinträchtigung gibt, liegen vor, wenn:

- LLMoin genutzt wird, um in einem Verfahren eine **eng gefasste Aufgabe zu erfüllen**, wie etwa unstrukturierte Daten in strukturierte Daten umzuwandeln, eingehende Dokumente in Kategorien einzuordnen oder zur Erkennung von Duplikaten. Diese Aufgaben sind so eng gefasst und begrenzt, dass sie nur beschränkte Risiken darstellen, die sich durch die Verwendung von LLMoin in einem Kontext, der in einem Anhang III der KIVO als Verwendung mit hohem Risiko aufgelistet ist, nicht erhöhen.
- LLMoin das **(Zwischen-)Ergebnis einer menschlichen Tätigkeit lediglich verbessert**, die für die Zwecke einer Verwendung mit hohem Risiko relevant sein kann. Unter Berücksichtigung dieser Merkmale wird eine menschliche Tätigkeit durch LLMoin lediglich durch eine zusätzliche Ebene ergänzt und stellt daher ein geringeres Risiko dar. Dies ist der Fall, wenn LLMoin genutzt wird, um die von Menschen in Dokumenten verwendete Sprache zu verbessern, etwa den professionellen Ton, den wissenschaftlichen Sprachstil oder um den Text an einen bestimmten Stil anzupassen.
- mit LLMoin menschlich generierte **Entscheidungsmuster** oder Abweichungen von früheren menschlich generierten Entscheidungsmustern **erkannt werden sollen**. Das Risiko wäre geringer, da LLMoin einer zuvor abgeschlossenen menschlichen Bewertung folgt, die ohne angemessene menschliche Überprüfung nicht ersetzt oder beeinflusst werden soll. Zum Beispiel, wenn LLMoin eingesetzt wird, um zu prüfen, ob von Bewertungsmustern abgewichen wurde, um so auf mögliche Unstimmigkeiten oder Unregelmäßigkeiten aufmerksam zu machen.<sup>2</sup>

- LLMoin genutzt wird, um eine Aufgabe auszuführen, die eine **menschliche Bewertung lediglich vorbereitet**, wodurch die mögliche Wirkung des Ergebnisses von LLMoin im Hinblick auf das Risiko für die folgende Bewertung sehr gering bleibt. Diese Bedingung umfasst u. a. intelligente Lösungen für die Bearbeitung von Dossiers, wozu verschiedene Funktionen wie Indexierung, Suche, Text- und Sprachverarbeitung, Verknüpfung von Daten mit anderen Datenquellen oder die Übersetzung von Erstdokumenten gehören.<sup>3</sup>

Eine Nutzung von LLMoin in nachstehenden **beispielhaften** Fallkonstellationen würde hingegen in den Anwendungsbereich von Anhang III fallen **und** eine wesentliche Beeinträchtigung von Gesundheit, Sicherheit und Grundrechten darstellen und ist somit **untersagt**.

- Die automatische (Vor-)Auswahl eines Kandidaten für eine Stelle basierend auf einer von LLMoin erstellten Rangliste.
- Die Übernahme von LLMoin vorgeschlagenen juristischen Argumenten ohne detaillierte menschliche Prüfung in ein Gerichtsurteil oder Verwaltungsentscheidung.
- Die ungeprüfte Übernahme einer von LLMoin getroffenen Entscheidung über die Gewährung von Sozialleistungen.
- LLMoin erstellt Risikoprofile zur Betrugsprävention im Bereich Sozialleistungen.

## Anhang zu Schutz von Rechten Dritter

Beim Einsatz von LLMoin müssen immer die Rechte Dritter beachtet werden. Auch wenn die Eingaben in LLMoin nicht für Trainingszwecke verwendet oder dauerhaft gespeichert werden, können die von LLMoin erzeugten Ausgaben später zu Rechtsverletzungen führen.

Wenn die Eingabe beispielsweise urheberrechtlich geschützte Inhalte oder Betriebs- und Geschäftsgeheimnisse enthält, muss bei der Verwendung der Ausgabe besonders darauf geachtet werden, dass keine Rechte verletzt werden.

Da Trainingsdaten von LLMs in den Ausgaben in der Regel nicht reproduziert werden, sind Urheberrechtsverletzungen unwahrscheinlich. Eine Urheberrechtsverletzung kann jedoch dann vorliegen, wenn die Verarbeitung von geschützten Inhalten in LLMoin dem ursprünglichen Werk zu ähnlich ist. Zum Beispiel, wenn LLMoin gebeten wird, einen urheberrechtlich geschützten Text zu reproduzieren oder in eine andere Sprache zu übersetzen, könnten Urheberrechte verletzt werden. Bei der Nutzung des KI-generierten Ergebnisses ist zu prüfen, ob und inwieweit vorbestehende Werke darin erkennbar sind.

Außerdem ist es verboten, Unternehmensdaten, die nicht öffentlich sind und deren Nichtverbreitung im Interesse des Unternehmens liegt, zu veröffentlichen. Wenn solche Daten nach der Verarbeitung in LLMoin (z.B. Zusammenfassung, Strukturierung von Daten, Textgenerierung) noch erkennbar sind, darf die Ausgabe nicht so verwendet werden, dass die Daten an Außenstehende oder die Öffentlichkeit weitergegeben werden könnten.