KI und Datenschutz: So führt eine Aufsichtsbehörde KI selbst ein

Von Glieks-Redaktion · Veröffentlicht am 18.11.2026

Hamburgs Datenschutzbehörde beschreibt, wie sie einen KI-Chatbot prüfte und selbst nutzt - mit Schutzmaßnahmen, Grenzen und Regeln. Was kleine Betriebe und Vereine daraus für ihren Alltag lernen können.

4.220 Beschwerden und eine Frage

Eine Datenschutzbehörde prüft, ob andere sich an die Regeln halten. Wenn sie selbst KI einsetzt, wird die Sache besonders genau beobachtet. Der Hamburgische Datenschutzbeauftragte hat das in einer zehnseitigen Fallstudie vom 5. November 2026 offengelegt. Im Jahr 2025 gingen bei der Behörde 4.220 Beschwerden ein, 62 Prozent mehr als im Vorjahr, und 2026 steigt die Zahl in ähnlichem Maß weiter, ohne dass im gleichen Umfang Personal hinzukam [1].

Deshalb nutzt die Behörde den KI-Assistenten LLMoin der Hamburger Verwaltung, nachdem sie dessen Einführung selbst aufsichtsrechtlich geprüft und das Ergebnis als positiv bewertet hat [1]. Die Fallstudie ist keine Rechtsnorm und kein Urteil. Der Beauftragte sagt selbst, dass andere Aufsichten oder Gerichte abweichen können [1].

Die Schutzmaßnahmen im Überblick

Die Behörde stützt sich auf eine Stellungnahme des Europäischen Datenschutzausschusses von Dezember 2024 und geht pragmatisch davon aus, dass ein Sprachmodell wahrscheinlich nicht anonym ist. Deshalb zählt, was das System rund um das Modell leistet. Genannt werden Filter für Eingaben und Ausgaben, ein Systemprompt mit Grundanweisungen, die Anbindung an geprüfte Quellen für die Recherche, verbindliche Nutzungsregeln, ein beauftragtes Red Teaming, bei dem das System gezielt mit heiklen Eingaben getestet wird, sowie Schulungen [1].

Besonders aufschlussreich sind die Grenzen: Der Systemprompt gilt ausdrücklich nicht als Ersatz für technische Schutzmaßnahmen, und Filter zählen nicht als Löschung im Sinne der DSGVO. Das nachträgliche Entfernen von Wissen aus einem Modell gilt nach der Fallstudie als Forschungsfeld ohne technische Reife [1].

Schritt für Schritt statt alles auf einmal

Die Einführung in der Behörde lief in Phasen. Zuerst durfte LLMoin nur ohne Personenbezug genutzt werden, etwa für Artikel im Tätigkeitsbericht oder für Zusammenfassungen anonymisierter Gerichtsentscheidungen. Danach wurden mit einer Testgruppe Vorlagen für typische Schreiben entwickelt, zunächst mit erfundenen, dann mit echten Fallakten, begleitet von einer Schulung zu Halluzinationen und zu den Grenzen der KI. Erst danach folgte der Betrieb für Akten mit normalem Schutzbedarf [1].

Klare Grenzen gelten weiter: Das System darf keine Beschwerden entscheiden und keine rechtlichen Bewertungen vornehmen. Die Fachleute lesen die Akte vollständig, legen die Kernargumente fest, und LLMoin hilft nur bei Formulierung und Gliederung. Beschwerden mit besonders sensiblen Daten, etwa aus

einer Psychotherapiepraxis, werden derzeit ausschließlich von Menschen bearbeitet. Rechtsbehelfsbelehrungen lässt die Behörde bewusst nicht von der KI formulieren, weil der Wortlaut exakt stimmen muss [1].

Eine Rolle spielt auch das Schufa-Urteil des Europäischen Gerichtshofs von 2023: Aus ihm lässt sich nach Auffassung des Hamburger Beauftragten ableiten, dass KI-generierte Vorschläge selbst dann als automatisierte Entscheidung gelten können, wenn ein Mensch sie später beurteilt, sofern sie dafür eine maßgebliche Rolle spielen. Deshalb lässt die Behörde das System keine rechtlichen Bewertungen vornehmen und mahnt zur Wachsamkeit gegenüber Automationsbias [1].

Orientierungshilfen für alle

Die Datenschutzkonferenz des Bundes und der Länder hat bereits im Mai 2024 eine Orientierungshilfe veröffentlicht, die ausdrücklich als Checkliste für Unternehmen, Behörden und andere Organisationen gedacht ist. Sie behandelt Zweckbestimmung, Transparenz, Betroffenenrechte und die Richtigkeit von Ergebnissen [2]. Im Juni 2025 folgte ein Papier zu technischen und organisatorischen Maßnahmen, das sich vor allem an Hersteller richtet [4]. Für die Bundesverwaltung gibt es seit Dezember 2025 außerdem eine Handreichung des Bundesbeauftragten, die einen risikobasierten Ansatz verfolgt [1][3].

Wussten Sie schon?

Der Content-Filter von LLMoin sortiert Ausgaben nach den Kategorien Hass, Sexualität, Gewalt und Selbstverletzung und unterdrückt entsprechende Inhalte [1].

Die Behörde hält eine Kennzeichnung jedes einzelnen Schreibens als KI-vorformuliert rechtlich für nicht notwendig, informiert aber in ihrer Datenschutzerklärung über den Einsatz [1]. Ein Filter gilt nach Auffassung der Datenschutzkonferenz nicht als Löschung im Sinne der DSGVO [1].

Was Sie sich für Ihren Betrieb oder Verein abschauen können

Auch ohne Behörde lassen sich die Ideen aufgreifen: erst mit unkritischen Texten üben, vorher festlegen, wofür KI genutzt wird und was nicht hineingehört, sensible Fälle ausnehmen und jedes Ergebnis vor dem Versand lesen. Ein kleines Verzeichnis, welche Werkzeuge im Betrieb genutzt werden und welche Daten dort eingegeben werden dürfen, schafft Überblick. Dies ersetzt keine Rechtsberatung. Fragen zur eigenen Lage klären Sie bitte mit Ihrer Datenschutzberatung oder der zuständigen Aufsichtsbehörde.

> **Merken Sie sich:** Wer KI einführt, fängt mit unkritischen Texten an, legt Regeln fest, nimmt sensible Fälle aus und lässt jedes Ergebnis von einem Menschen prüfen [1].

Was Glieks für Ihren Datenschutz-Alltag tun kann

- **Regeln für KI im Betrieb** - Ein einseitiges Regelblatt als Word-Dokument.
- **Werkzeug-Verzeichnis anlegen** - Eine Excel-Tabelle, welche Werkzeuge mit welchen Daten genutzt werden.
- **Fragen an den Anbieter sammeln** - Eine Fragenliste, die Sie einem KI-Anbieter stellen können.

Direkt ausprobieren: https://glieks.ai/glieks-news/ki-und-datenschutz-aufsicht

Quellen

1. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: Fallstudie: KI-Chatbot LLMoin (Stand: 05.11.2026, abgerufen am 18.11.2026)
2. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK): Künstliche Intelligenz datenschutzkonform einsetzen: Datenschutzkonferenz veröffentlicht Orientierungshilfe für Unternehmen und Behörden (Stand: 06.05.2024, abgerufen am 18.11.2026)
3. zm-online: KI kommt jetzt auch in die Verwaltung (Stand: 18.02.2026, abgerufen am 18.11.2026)
4. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK): Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen, Version 1.0 (Stand: Juni 2025, abgerufen am 18.11.2026)

Diesen Beitrag online lesen: https://glieks.ai/glieks-news/ki-und-datenschutz-aufsicht

Angaben ohne Gewähr. Die Glieks-News fassen öffentlich zugängliche Quellen in eigenen Worten zusammen. Keine Rechts-, Steuer- oder Anlageberatung - maßgeblich sind die verlinkten Quellen. Dieser Beitrag entstand mit KI-Unterstützung auf Grundlage der genannten Quellen.