

Kommunale KI-Nutzung leicht gemacht: Technik, Recht und IT-Sicherheit im Überblick

– Arbeitspapier –

Dr. Neven Josipovic

Braunschweig, 11.12.2025

Abstract

Das Arbeitspapier vermittelt grundlegendes Wissen über den Einsatz von künstlicher Intelligenz (KI) in Kommunalverwaltungen und stellt Anwendungsfelder wie Chatbots, automatisierte Protokollerstellung und KI-gestützte Dokumentenrecherche vor. Es analysiert technische Umsetzungsoptionen – von öffentlich zugänglichen KI-Systemen über Software-Dienste bis hin zu Cloud-Plattformen – und deren Vor- und Nachteile. Ein besonderer Fokus liegt auf den rechtlichen und organisatorischen Rahmenbedingungen, darunter die EU KI-Verordnung, das Datenschutzrecht, die Mitbestimmungsrechte der Personalvertretung sowie mögliche Inhalte interner Regelungen. Ergänzend werden Anforderungen an die IT-Sicherheit und Maßnahmen zur sicheren Nutzung generativer KI-Modelle erläutert. Der Text bietet Kommunen eine praxisorientierte Grundlage, um wesentliche Aspekte der kommunalen KI-Nutzung zu verstehen und eigene KI-Projekte umzusetzen.

Inhalt

| | |
|---|-----------|
| Einleitung | 3 |
| 1. Ausgangslage | 3 |
| 2. Ziele des Arbeitspapiers | 3 |
| 3. Überlegungen zur Methodik | 4 |
| I. Begriffsbestimmungen | 7 |
| II. KI-Grundlagen am Beispiel von ChatGPT | 8 |
| III. Einsatzfelder für KI in der öffentlichen Verwaltung | 10 |
| 1. Darstellung von Anwendungsfällen | 10 |
| a. Allgemeine KI-Assistenten/Chatbots | 11 |
| b. Bürger-Service-Chatbots..... | 11 |
| c. Automatisierte Protokollerstellung | 11 |
| d. KI-Unterstützung in Antragsprozessen..... | 11 |
| e. Dokumentenrecherche mittels KI | 11 |
| f. KI-basierte Datenauswertung..... | 12 |
| 2. Zwischenfazit | 12 |
| IV. Möglicher Einstieg in die kommunale KI-Nutzung | 13 |
| 1. Optionen für die technische Implementierung..... | 13 |
| a. Öffentlich zugängliche KI-Systeme..... | 13 |
| b. Beschaffung als Software-Dienst | 14 |
| c. Bereitstellung von KI über Cloud-Plattformen..... | 15 |
| 2. Zwischenfazit | 17 |
| V. IT-Sicherheit | 18 |
| 1. BSI-Schichtenmodell bei kommunalen KI-Projekten..... | 18 |
| 2. Spezielles BSI-Material zum Einsatz von KI | 19 |
| a. Maßnahmen zur Risikominderung bei generativer KI | 19 |
| b. BSI-Kriterienkatalog für generative KI | 21 |
| 3. Zwischenfazit | 22 |
| VI. Rechtliche und organisatorische Aspekte | 23 |
| 1. Rechtlicher Rahmen, insb. EU KI-VO und Datenschutzrecht..... | 23 |
| a. Anforderungen der EU KI-VO an die kommunale KI-Nutzung | 23 |
| b. Datenschutzrechtliche Anforderungen | 26 |
| c. Mitbestimmungs- und Mitwirkungsrechte..... | 28 |
| 2. Mögliche Inhalte interner Regelungen | 29 |
| 3. Zwischenfazit | 31 |
| VII. Zusammenfassung | 32 |
| VIII. Fazit | 34 |
| Quellen | 35 |
| Anhang: Auszug aus dem BSI-Kriterienkatalog | 37 |

Einleitung

1. Ausgangslage

Künstliche Intelligenz (KI) erhält Einzug in immer mehr Bereiche des digitalen Lebens und Arbeitens. Menschen nutzen sie als eigenständige Anwendungen, etwa als Chatbots oder Assistenten, und Unternehmen integrieren sie in immer mehr Produkte und Prozesse. Insgesamt zeichnet sich ein technologischer Trend ab, bei dem Menschen immer mehr Tätigkeiten an KI-Systeme delegieren.

Auch Kommunalverwaltungen sind von diesem Trend betroffen. Im Kontext laufender Digitalisierungsaktivitäten und im Spannungsfeld zwischen einer zunehmenden Aufgabendichte und einem Mangel an Fachkräften könnte KI ein zusätzlicher Baustein sein, um den Herausforderungen zu begegnen.

Laut einer Studie aus dem Jahr 2024 sind durch den Einsatz von generativer KI im öffentlichen Sektor Produktivitätseffekte von bis zu rund 440 Mrd. Euro möglich.¹ Schätzungsweise bis zu 85 % administrativer Aufgaben lassen sich mit Hilfe von generativer KI automatisieren, die Fachkräftelücke in der öffentlichen Verwaltung durch einen flächendeckenden KI-Einsatz um ein Drittel verkleinern.²

Gleichzeitig wird deutlich, dass sich Mitarbeiterinnen und Mitarbeiter der Vorteile von KI für ihren Arbeitsalltag bewusst sind und die Vorteile auch nutzen. Beispielsweise wird geschätzt, dass fast jeder zweite Mitarbeiter (45 %) in Politik und Verwaltung auf Bundesebene KI-Tools nutzt, die nicht von ihrer Organisation geprüft und als sicher eingestuft wurden.³

Fest steht, dass sich Kommunalverwaltungen mit dem Thema KI beschäftigen müssen. Derzeit mangelt es jedoch an Hilfsmaterial, das die verschiedenen Aspekte, die mit dem Einsatz von KI zusammenhängen, aufbereitet und interessierten Verwaltungen eine Orientierung für den Einstieg in eigene Pilotprojekte bietet.

2. Ziele des Arbeitspapiers

Das Arbeitspapier zielt darauf ab, häufig in Kommunen auftretende Fragen zum Einsatz von KI zu beantworten, für den kommunalen Einsatz von KI relevante Informationen zu aggregieren und Kommunen dadurch in die Lage zu versetzen, zu ihren Bedarfen und Randbedingungen passende KI-Projekte zu planen und umzusetzen.

Da KI ein Überbegriff für verschiedene Konzepte ist, widmet sich der erste Abschnitt der Definition relevanter Begriffe. Der zweite Abschnitt erläutert am Beispiel von ChatGPT die grundlegende Funktionsweise von KI-Modellen, insbesondere großen Sprachmodellen.

Im dritten Abschnitt werden ausgewählte in Kommunal- und Landesverwaltungen in der Erprobung befindliche Anwendungsfälle für KI dargestellt. Auf der Grundlage beschreibt der vierte Abschnitt einen möglichen Einstieg in die kommunale KI-Nutzung, wobei der Fokus darauf liegt, die Vor- und Nachteile verschiedener technischer Umsetzungsvarianten zu klären.

¹ McKinsey, GenAI, 2024, S. 1.

² Ebd., S. 2, 6.

³ Microsoft, Schatten-KI, 2025.

Im fünften Abschnitt wird die Frage beantwortet, welche grundlegenden Anforderungen an die Gewährleistung von IT-Sicherheit bestehen und anhand welcher Materialien Kommunen die IT-Sicherheit in KI-Projekten bewerten können.

Der sechste Abschnitt klärt, welche rechtlichen Anforderungen bestehen, die Kommunen bei der Planung und Durchführung von KI-Projekten zu beachten haben. Darüber hinaus wird in dem Abschnitt aufgezeigt, welche Aspekte im Zusammenhang mit der KI-Nutzung Kommunen in internen Regelungen festlegen können.

3. Überlegungen zur Methodik

Das Arbeitspapier erhebt keinen Anspruch an Vollständigkeit. Es orientiert sich an Fragen, die insbesondere in kleineren und mittelgroßen Kommunen aufkommen, wenn sie sich erstmalig mit dem Thema künstliche Intelligenz befassen und die Technologie erproben möchten.

Die Erläuterungen in den ersten beiden Abschnitten dienen primär dazu, in kondensierter Weise ein Verständnis der technischen Grundlagen zu vermitteln. Beispielsweise ist es hilfreich, den Begriff der großen Sprachmodelle zu kennen und im Kontext von KI einordnen zu können, da diese Variante aufgrund ihrer Flexibilität und Leistungsfähigkeit häufig in kommunalen Einsatzfeldern verwendet wird. Die Beschreibung der Funktionsweise von großen Sprachmodellen am Beispiel von ChatGPT zielt darauf ab, ein Verständnis für die wahrscheinlichkeitsbasierte Funktionsweise von generativen KI-Modellen sowie damit einhergehende Kenntnisse über ihre Fähigkeiten und Herausforderungen zu vermitteln. Letztere betreffen Halluzinationen und mögliche Vorprägungen von KI-Modellen, die auf die verwendeten Trainingsdaten und menschlicher Mitwirkung im Trainingsprozess zurückzuführen sind.

Der dritte Abschnitt soll Kommunen ein konkretes Bild darüber vermitteln, welche KI-Anwendungen in Kommunal- und Landesverwaltungen verwendet werden. Die beschriebenen Anwendungsfälle umfassen sowohl Erprobungs- und Pilotanwendungen als auch KI-Nutzungen, die bereits in eine Phase der Verstetigung bzw. des Dauerbetriebs übergegangen sind.

Auf der Grundlage klärt der vierte Abschnitt die Frage, welche technischen Wege Kommunen offen stehen, um KI-Modelle in eigene kommunale Projekte zu integrieren. Für die technische Umsetzung bestehen prinzipiell vier Optionen, die verschiedene Vor- und Nachteile aufweisen:

- Nutzung im Internet öffentlich zugänglicher KI-Systeme,
- Beschaffung als Software-Dienst,
- Bereitstellung von KI über Cloud-Plattformen,
- Lokaler Betrieb von Open-Source-Modellen.

Eine zentrale Herausforderung bei allen Varianten besteht darin, dass KI-Modelle – wie beispielsweise große Sprachmodelle – eine derart große Rechenleistung erfordern, dass sie häufig nicht von Kommunen selbst betrieben, sondern über externe Dienste (*Cloud*) angebunden werden müssen. Das bedeutet, dass Kommunen, die KI-Systeme nutzen möchten, im Regelfall nicht darum herum kommen, sich mit den Besonderheiten der externen Verarbeitung von Daten auseinanderzusetzen.

Aufgrund von Limitationen bei Ressourcen und den erforderlichen IT-Kenntnissen werden Kommunen nur in Ausnahmefällen alle für die Nutzung von KI erforderlichen Hard- und Softwarekomponenten lokal installieren und betreiben können (*On-premise*). Dennoch lässt sich ein Eigenbetrieb erfolgreich realisieren. Diese Umsetzungsoption ist beispielsweise dann re-

levant, wenn besonders sensible und vertrauliche Daten und Dokumente indiziert und verarbeitet werden sollen und Anforderungen an die Datensicherheit daher andere Faktoren wie Kosten für IT-Infrastruktur, Aktualität der KI-Modelle, automatische Systemupdates, technischen Support und einfache Skalierbarkeit überwiegen.

Da der lokale Betrieb von KI-Systemen für die meisten Kommunen derzeit aus den genannten Gründen nicht realisierbar ist, wird diese Variante im vorliegenden Arbeitspapier nicht behandelt.

Der fünfte Abschnitt behandelt das Thema IT-Sicherheit. Prinzipiell sind KI-Systeme wie IT-Systeme zu betrachten und unterliegen denselben Vorgaben für die IT-Sicherheit.⁴ Eine für Kommunalverwaltungen relevante Quelle für Informationen und Empfehlungen auf dem Gebiet ist das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Die Informationen des BSI sind für Kommunalverwaltungen besonders relevant, da es als staatliche und auf IT-Sicherheit spezialisierte Einrichtung neutrale Empfehlungen und anerkannte Standards erarbeitet und über umfassende und auf behördliche Anforderungen zugeschnittene Expertise verfügt. Aus dem Grund wird im Abschnitt zur IT-Sicherheit anhand von Material des BSI geprüft, welche Anforderungen an IT-Sicherheit bestehen, wenn Kommunen KI – und insbesondere generative KI – einsetzen möchten. Geklärt wird auch, welche Maßnahmen die Literatur des BSI vorsieht, um Risiken im Zusammenhang mit der KI-Nutzung zu reduzieren.

Im sechsten Abschnitt geht es darum, wesentliche für den kommunalen KI-Einsatz relevante gesetzliche Anforderungen darzustellen und ihre Implikationen für KI-Projekte zu klären. Allgemein können in kommunalen KI-Projekten Vorschriften aus dem folgenden Bereichen zu beachten sein:⁵

- Verordnung (EU) 2024/1689 („KI-Verordnung“),
- Gesetzliche Anforderungen an den Datenschutz,
- Mitbestimmungs- und Mitwirkungsrechte der Personalvertretung,
- Spezielle landesrechtliche Vorschriften über den Einsatz von KI,
- Urheberrechtliche Vorgaben,
- Regelungen über automatisierte Verwaltungsentscheidungen,
- Anforderungen an die Wahrung von Dienstgeheimnissen,
- Anforderungen an materiellen Geheimschutz und IT-Sicherheit,
- Zusätzliche technische und organisatorische Anforderungen bei Verarbeitung sensibler Daten (z.B. Steuerdaten).

Zwei Rechtsgebiete, die im Kontext von KI häufig Fragen in Kommunen aufwerfen, sind zum einen das Unionsrecht – namentlich die EU-Verordnung 2024/1689 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz („EU KI-Verordnung“) – und das Datenschutzrecht. Aus diesem Grund liegt der Schwerpunkt des Arbeitspapiers auf diesen beiden Bereichen. Darüber hinaus wird summarisch auf die Vorschriften über die Mitwirkung und Mitbestimmung der Personalvertretung eingegangen.

Beim Datenschutzrecht ist anzumerken, dass Kommunen an den Vorgaben der Datenschutz-Grundverordnung (DS-GVO) und der Landesdatenschutzgesetze zu entsprechen haben. Die

⁴ StMFH Bayern, KI-Leitfaden, 2025, S. 31.

⁵ Ebd., S. 10.

DS-GVO ist die zentrale Datenschutzregelung in der Union und gilt unmittelbar in allen Mitgliedstaaten. Die Landesdatenschutzgesetze ergänzen die DS-GVO um landesspezifische Anforderungen.

Da die DS-GVO die allgemeinen Grundsätze und Anforderungen für die Verarbeitung personenbezogener Daten festlegt und auch für Kommunen gilt, die KI-Projekte umsetzen, liegt auf ihr der Schwerpunkt bei der Klärung datenschutzrechtlicher Vorgaben.

Im Hinblick auf die Abschnitte zum rechtlichen Rahmen ist anzumerken, dass keine eigene Auslegung von Tatbestandsmerkmalen erfolgt, sondern die Literatur zu dem Thema herangezogen wird. Zentrale Quellen sind dabei die Veröffentlichungen der Kommunalen Gemeinschaftsstelle für Verwaltungsmanagement (KGSt) zum Thema KI sowie der Leitfaden für bayerische Behörden zum Einsatz von Künstlicher Intelligenz in der Staatsverwaltung des Bayerischen Staatsministeriums der Finanzen und für Heimat (StMFH).

Zuletzt geht es im sechsten Abschnitt um die Frage, welche Inhalte Kommunen in internen Regelungen wie Dienstanweisungen und Dienstvereinbarungen vorsehen können. Anhand von Erfahrungen aus der Praxis und Ansichten in der Literatur werden hier mögliche Klauseln vorgestellt, an denen sich Kommunen bei der Entwicklung eigener Regelungen wie Dienstanweisungen und Dienstvereinbarungen orientieren können.

I. Begriffsbestimmungen

Künstliche Intelligenz steht für informationstechnische Systeme, die Aufgaben erledigen können, die üblicherweise menschliche Intelligenz erfordern. Solche Systeme basieren auf Algorithmen und statistischen Modellen, um aus Daten zu lernen und (teil-)autonom zu agieren.

Die Fähigkeiten von KI nehmen stetig zu, was daran zu erkennen ist, dass KI in immer mehr Bereichen einen Gleichstand mit menschlichen Fähigkeiten erreicht – so etwa auf den Gebieten Sprachverständnis⁶, Übersetzungen⁷ sowie Beschreibung⁸ und Klassifizierung⁹ von Bildern.

Künstliche Intelligenz ist ein Oberbegriff für verschiedene Konzepte. Sie lassen sich anhand der historischen Entwicklung von KI beschreiben.

Frühe Systeme basierten auf Algorithmen mit vordefinierten Regeln und waren nicht lernfähig. Mit der Entwicklung von Algorithmen, die aus Daten lernen und Muster erkennen konnten, entstand das Gebiet des *maschinellen Lernens (ML)*. Dabei werden Algorithmen darauf ausgelegt, Muster und Korrelationen in großen Datensätzen zu erkennen, um auf der Grundlage Vorhersagen zu treffen.¹⁰

Zunehmende Datenmengen und Rechenleistung führen zum sogenannten *tiefen Lernen (Deep Learning, DL)*, einer Form des maschinellen Lernens, die zunehmend auf künstlichen *neuronalen Netzen* basiert. Die Vielschichtigkeit der zugrundeliegenden Modelle erlaubte immer umfassendere und komplexere Ein- und Ausgaben, was die Leistungsfähigkeit von KI deutlich erhöhte.

Seit der Jahrtausendwende gewann der Bereich der *generativen KI (GenAI)* an Bedeutung. Sie basiert auf tiefem Lernen, legt den Fokus aber nicht auf Analyse und Prognose, sondern auf die praktische Anwendung zur Erstellung von Inhalten. Bei generativer KI geht es darum, Inhalte zu erstellen oder zu synthetisieren, die zwar den Trainingsdaten ähneln, aber einzigartig sein sollen.

Ein wichtiger Schritt im Bereich des tiefen Lernens waren *große Sprachmodelle (Large Language Models, LLM)*. Diese Modelle auf Grundlage neuronaler Netze werden insbesondere darauf trainiert, menschliche Sprache zu verstehen und zu generieren. Sie nutzen umfangreiche Datensätze, um Muster in Texten zu erkennen und darauf basierend kohärente und kontextbezogene Antworten zu generieren.

Ein bekanntes Beispiel für die Anwendung eines großen Sprachmodells ist ChatGPT. Es basiert auf einer Reihe fortschrittlicher, multimodaler Modelle, die natürliche Sprachen verstehen und generieren zunehmend auch visuelle und auditive Daten verarbeiten können.

⁶ Xiong et al., 2017.

⁷ Hassan et al., 2018.

⁸ Hu et al., 2021.

⁹ He et al., 2015.

¹⁰ SAP, Machine Learning, 2025.

II. KI-Grundlagen am Beispiel von ChatGPT

Dieser Abschnitt dient dazu, in kondensierter Weise ein Verständnis der technischen Grundlagen von großen Sprachmodellen zu vermitteln, da diese Variante von KI-Modellen aufgrund ihrer Flexibilität und Leistungsfähigkeit häufig für kommunale KI-Anwendungen genutzt wird.¹¹

GPT-Sprachmodelle sind in der Lage, logische Zusammenhänge zwischen Sätzen und Konzepten zu erkennen, Fragen zu beantworten, unterschiedliche Bedeutungen von Begriffen zu differenzieren und Texte einzuordnen. Neuere Versionen, beginnend mit GPT-4 bis zum aktuellen GPT-5, sind multimodal. Das bedeutet, sie akzeptieren als Eingabe nicht nur Text, sondern auch Bilder, Text/Bild-Kombinationen, Audioeingaben und können Sprachkonversationen in Echtzeit führen.

Durch ein Vortraining, insbesondere mit großen Datenmengen aus dem Internet, erwerben die Modelle selbstständig Allgemeinwissen und lernen, sprachliche und inhaltliche Zusammenhänge zu verstehen. Die Feinabstimmung der Modelle erfolgt unter anderem durch *Reinforcement Learning from Human Feedback (RLHF)*. Dabei teilen Menschen dem Modell mit, welche Reaktionen als „richtig“, nützlich und sicher erachtet werden, um das Antwortverhalten des Modells an menschliche Erwartungen anzupassen.

Bei der GPT-Reihe handelt es sich um Sprachmodelle, die darauf ausgelegt sind, den nächsten *Token* – also Wort oder Wortteil – vorherzusagen und die statistisch wahrscheinlichste und kohärenteste Antwort zu liefern. Dieses Merkmal der Vorhersage wahrscheinlicher Fortsetzungen bei großen Sprachmodellen kann dazu führen, dass sie Fakten erfinden oder falsche Informationen generieren (*halluzinieren*). Der Fehlerquotient reduziert sich zwar mit jeder neuen Modelliteration, stellt aber nach wie vor eine Herausforderung für den Einsatz der Modelle dar und muss bei der Konfiguration von KI-Modellen berücksichtigt werden.

Halluzinationen in KI-Systemen stellen ein Problem dar, da sie in mehreren Bereichen negative Auswirkungen haben können. Wenn KI-Modelle falsche oder irreführende Informationen liefern, kann dies das Vertrauen der Nutzer in die Technologie untergraben und ihre Akzeptanz mindern.¹²

Besonders kritisch wird es, wenn KI-Systeme in sensiblen Bereichen wie Finanzen, Gesundheitswesen oder Recht eingesetzt werden, da ungeprüfte Ausgaben, die fehlerhafte Informationen enthalten, zu schwerwiegenden Fehlentscheidungen führen können. Schließlich bergen inhaltliche Ungenauigkeiten auch rechtliche Risiken, da sie Entwickler und Nutzer der KI-Systeme einer möglichen Haftung aussetzen können.

Eine weitere Herausforderung für den Einsatz von großen Sprachmodellen hat ihre Ursache darin, dass sie anhand großer Datenmengen, die zum überwiegenden Teil dem Internet entstammen, trainiert werden. Dadurch können die Modelle Voreingenommenheiten aus den Trainingsdaten übernehmen. Andererseits kann die menschliche Feinabstimmung der Modelle, die Voreingenommenheiten reduzieren soll, dazu führen, dass sie sich weigern, Anfragen zu bearbeiten, die gegen Sicherheitsrichtlinien verstoßen.

¹¹ Vgl. die Überlegungen zur Methodik in der Einleitung.

¹² Marr, Hallucinations, 2023.

Da sich Modelle verschiedener Anbieter in ihrer Datenbasis und Feinabstimmung deutlich unterscheiden können, wird die Auswahl des passenden KI-Modells für den jeweiligen kommunalen Anwendungsfall immer wichtiger.

Die genannten Herausforderungen ändern nichts an der Tatsache, dass die Leistungsfähigkeit moderner KI-Modelle in vielen Bereichen ein Niveau erreicht hat, das mit menschlichen Fähigkeiten vergleichbar ist oder diese sogar übertrifft. GPT-4 und GPT-5 zeigen bei einer Vielzahl von akademischen Prüfungen, die ihnen zuvor unbekannt waren, Ergebnisse, die mit den besten menschlichen Testteilnehmern konkurrieren können. So bestand GPT-4 beispielsweise das US-amerikanische Juristische Examen (Uniform Bar Examination) mit einer Punktzahl, die zu den besten 10 % der Teilnehmer zählt.

Die Modelle sind zudem multilingual und bewältigen Aufgaben in verschiedenen Sprachen, darunter Deutsch, Englisch, Französisch, Spanisch und Chinesisch, mit beeindruckender Kompetenz. Darüber hinaus sind neue Modelle wie GPT-5 in der Lage, nicht nur Texte, sondern auch Bilder, Diagramme und Audioeingaben zu erkennen, zu verstehen und nahtlos zu integrieren. Sie können Dokumente mit komplexen Layouts ebenso verarbeiten wie Echtzeit-Sprachbefehle. Aufgrund dieser Fähigkeiten bieten große Sprachmodelle viel Potenzial, in unterschiedlichen Bereichen der öffentlichen Verwaltung eingesetzt zu werden.

Zusammenfassend bedeutet das für Kommunen:

- Große Sprachmodelle können in kommunalen Anwendungen vielseitig eingesetzt werden, etwa zur Bearbeitung von Bürgeranfragen, zur Textgenerierung oder zur Analyse von Dokumenten in verschiedenen Sprachen und Formaten.
- Kommunen müssen Risiken wie Halluzinationen (falsche Informationen) oder Voreingenommenheiten berücksichtigen und Maßnahmen zur Qualitätssicherung und Überprüfung der Ergebnisse einplanen.

III. Einsatzfelder für KI in der öffentlichen Verwaltung

Verschiedene Landes- und Kommunalverwaltungen nutzen KI zur Verbesserung der Kommunikation mit Bürgerinnen und Bürgern sowie zur Unterstützung von Mitarbeiterinnen und Mitarbeitern. Dabei lassen sich drei Kategorien an Anwendungsfällen identifizieren: Chatbots zur Verbesserung der Bürgerkommunikation, interne KI-Chatbots zur Unterstützung der Mitarbeiter, und weitere Anwendungsfälle wie die automatisierte Protokollerstellung oder Indizierung von Dokumenten (Abbildung 1).¹³

| Anwendungsfall | Name | Bereitsteller | Einsatzorte (Beispiele) |
|-------------------------|------------------------|--|-----------------------------|
| Bürger-Service-Chatbot | JOST | viind | Landkreis Osnabrück |
| | Hein Mück | Neuraflow | Bremerhaven |
| | Frag-den-Michel | DAI Labor (TU Berlin), Dataport | Hamburg |
| | WiDu | Cognigy.AI | Duisburg |
| | FALKO | NEXT Data Service AG | Falkensee |
| | Ulmer Spatz | Uniquehorns | Ulm |
| | Colon Sültemeyer | Assono | Bad Oeynhausen |
| | Dienstleistungsfinder | Landeshauptstadt München RIT/it@M KICC | München |
| | Govii | Govii | Flensburg |
| | Lumi | Aleph Alpha | Heidelberg |
| Interne Chatbots | NRW.GENIUS | IT.NRW | Land Nordrhein-Westfalen |
| | LLMoin | Dataport | Hamburg, Land Niedersachsen |
| | M365 Copilot Chat | Microsoft, IT.Niedersachsen | IT.Niedersachsen |
| | F13 | Aleph Alpha, InnoLab_bw, ZenDiS | Land Baden-Württemberg |
| | MUCGPT | Landeshauptstadt München RIT/it@M KICC | München |
| | Microsoft Azure OpenAI | Microsoft Azure OpenAI | Braunschweig |
| Weitere Anwendungsfälle | FINO – der bol FormBot | BOL Behörden Online Systemhaus GmbH | Braunschweig |
| | forml | forml GmbH | Hannover |
| | Parla | CityLAB Berlin | Berlin |
| | inspira_BIB | Landeshauptstadt München RIT/it@M KICC | München |
| | SpeechMind | SpeechMind | Heidelberg |
| | Scriba | straiqr.ai GmbH | Landkreis Lüchow-Dannenberg |
| | enaioGPT | OPTIMAL SYSTEMS GmbH | Soltau |

Abbildung 1: Beispiele für den Einsatz von KI in Kommunal- und Landesverwaltungen (Stand: Oktober 2025).

1. Darstellung von Anwendungsfällen

Konkrete Beispiele für KI-Anwendungen, die in der öffentlichen Verwaltung erprobt werden, umfassen:

- Allgemeine KI-Assistenten/Chatbots
- Bürger-Service-Chatbots
- Automatisierte Erstellung von Protokollen
- Unterstützung in Antragsprozessen
- Dokumentenrecherche
- Datenauswertung

Die sechs Anwendungsfälle werden im Folgenden zusammenfassend beschrieben.

¹³ Josipovic, Einsatz von LLM, 2025, S. 3.

a. Allgemeine KI-Assistenten/Chatbots

Mitarbeiterinnen und Mitarbeiter einer Kommunalverwaltung können allgemeine KI-Assistenten und Chatbots in einer Vielzahl von Anwendungsbereichen einsetzen, um ihre tägliche Arbeit effizienter und produktiver zu gestalten. Die Assistenten unterstützen beispielsweise bei der Erstellung, Bearbeitung und Zusammenfassung von Texten, wie Dienstanweisungen, Vorlagen, Berichten oder Redeentwürfen. Dabei können sie nicht nur Inhalte generieren, sondern auch bestehende Texte überarbeiten, vereinfachen oder an spezifische Zielgruppen anpassen. Durch den Einsatz allgemeiner KI-Assistenten können Kommunen ihre Mitarbeiter nicht nur im Arbeitsalltag unterstützen, sondern auch die Qualität und Geschwindigkeit der Verwaltungsarbeit verbessern.

b. Bürger-Service-Chatbots

Service-Chatbots können Bürger bei der Informationssuche und der Nutzung städtischer Dienstleistungen unterstützen. Sie beantworten häufig gestellte Fragen und liefern Informationen zu kommunalen Angeboten in einem natürlichen Dialog. Die Chatbots sind im Regelfall jederzeit verfügbar und ermöglichen eine schnelle und effiziente Interaktion, was die Zugänglichkeit und Benutzerfreundlichkeit für Bürger erhöht.

c. Automatisierte Protokollerstellung

Die automatische Protokollerstellung mittels KI kann Kommunalverwaltungen bei der Dokumentation von Sitzungen, Besprechungen und anderen Veranstaltungen unterstützen. Mithilfe von großen Sprachmodellen werden Gesprächsinhalte analysiert, transkribiert und zusammengefasst. Die Protokolle enthalten die wesentlichen Punkte, Beschlüsse und Aufgaben, die während der Sitzung besprochen wurden, und können individuell angepasst werden. Dies ermöglicht eine schnelle und präzise Dokumentation und reduziert den manuellen Aufwand für Mitarbeiter.

d. KI-Unterstützung in Antragsprozessen

In Antragsprozessen kann KI sowohl Mitarbeiter in Kommunalverwaltungen als auch Bürgerinnen und Bürger unterstützen. Intern kann KI die zuständigen Sachbearbeiter durch automatische Vorsortierung und Vorprüfung von Anträgen entlasten. Dabei werden eingereichte Unterlagen analysiert, auf Vollständigkeit geprüft und nach festgelegten Kriterien kategorisiert, was die Bearbeitung beschleunigt und den manuellen Aufwand reduziert. Für Bürger bietet eine KI-Assistenz zusätzliche Unterstützung, indem sie den Antragsprozess verständlicher und zugänglicher gestaltet. Die KI kann beispielsweise beim Ausfüllen von Formularen helfen, indem sie Eingaben in verschiedenen Sprachen ermöglicht und automatisch übersetzt. Zudem kann sie Fragen zu den Antragsinhalten beantworten und den Antragsteller Schritt für Schritt durch den Prozess führen, was die Benutzerfreundlichkeit erhöht und dafür sorgt, dass weniger Fehler oder Unklarheiten entstehen.

e. Dokumentenrecherche mittels KI

Die Dokumentenrecherche stellt einen erweiterten Anwendungsfall von Chatbots dar, bei dem die Wissensbasis der KI gezielt auf die Bedürfnisse der Kommunalverwaltung zugeschnitten wird. Hierbei können digital vorliegende Dokumente, wie beispielsweise PDF-Dateien, indiziert und für ein großes Sprachmodell zugänglich gemacht werden. Die KI kann dadurch gezielt

Informationen aus umfangreichen Dokumentensammlungen abrufen, die sie zur Bearbeitung der jeweiligen Anfrage benötigt. Mitarbeiter in der Verwaltung können so schnell und effizient auf relevante Inhalte zugreifen, ohne manuell in Dokumenten suchen zu müssen. Auch Bürger können prinzipiell von dieser Technologie profitieren, wenn sie etwa über einen KI-gestützten Chatbot gezielt Fragen zu öffentlich zugänglichen Dokumenten stellen können.

f. KI-basierte Datenauswertung

Die Datenauswertung mittels KI bietet Kommunalverwaltungen die Möglichkeit, große und komplexe Datenmengen zu analysieren und aufzubereiten. Mithilfe von KI-Systemen, die natürliche Sprache verstehen und verarbeiten können, lassen sich Daten aus verschiedenen Quellen – wie Geodaten oder strukturierte Tabellendaten – dialogbasiert analysieren. Dies ermöglicht eine intuitive Interaktion, die keine Programmierkenntnisse oder Expertise in der Datenanalyse erfordert und den Analyseprozess erheblich beschleunigen kann. KI-Systeme können Daten dabei nicht nur auswerten, sondern auch Unregelmäßigkeiten erkennen, diese beheben und die Ergebnisse dokumentieren und interpretieren.¹⁴ Für Kommunalverwaltungen ergeben sich hier zahlreiche Anwendungsbereiche, wie die Analyse von Bevölkerungsstatistiken, die Auswertung von Verkehrs- oder Umweltdaten oder die Optimierung von Verwaltungsprozessen.

2. Zwischenfazit

Kommunen steht schon heute ein breites Spektrum an KI-Anwendungsfällen zur Verfügung. Sie können KI-gestützte Chatbots einsetzen, um die Kommunikation mit Bürgern zu verbessern, häufig gestellte Fragen zu beantworten und den Zugang zu städtischen Dienstleistungen zu erleichtern. KI-Anwendungen wie die automatisierte Protokollerstellung oder die Unterstützung in Antragsprozessen können Mitarbeiter unterstützen, indem sie Routineaufgaben wie die Dokumentation oder die Vorsortierung von Anträgen effizienter gestalten. Die Dokumentenrecherche mit KI ermöglicht eine schnelle und gezielte Suche in umfangreichen Dokumentensammlungen, was sowohl Mitarbeitern als auch Bürgern den Zugriff auf relevante Informationen erleichtert. Zuletzt kann die KI-basierte Datenauswertung Kommunen dabei helfen, große Datenmengen wie Bevölkerungs- oder Umweltdaten zu analysieren und Unregelmäßigkeiten zu erkennen.

Fraglich ist, wie Kommunen, die bislang keine oder nur wenige Erfahrungen mit KI haben, eigene KI-Projekte auf den Weg bringen können.

¹⁴ Josipovic, KI-basierte Datenauswertung, 2023, S. 37.

IV. Möglicher Einstieg in die kommunale KI-Nutzung

Der Einstieg in die Nutzung von KI in Kommunalverwaltungen ist ein individueller Prozess, für den es keine universelle Lösung gibt. Welche KI-Anwendungen für eine Kommune sinnvoll und nützlich sind, hängt von verschiedenen Faktoren ab: der Größe der Kommune, den verfügbaren personellen und finanziellen Ressourcen, dem vorhandenen IT-Know-how, dem aktuellen Stand der Digitalisierung sowie den spezifischen Prozessen, Strukturen und Bedürfnissen vor Ort. Dennoch gibt es grundlegende Prinzipien, die Kommunen bei der Einführung von KI-Technologien unterstützen können. Ein zentraler Aspekt ist, erste Erfahrungen mit der Implementierung und Nutzung von KI zu sammeln. Gleichzeitig müssen Strukturen und Prozesse geschaffen werden, die den systematischen Einsatz von KI fördern.

Ein sinnvoller Ansatz für den Einstieg in die kommunale KI-Nutzung ist die Durchführung von Pilotprojekten. Pilotprojekte ermöglichen es Kommunen, KI-Lösungen in einem begrenzten Rahmen zu testen und dabei Erkenntnisse über die technische Implementierung, die Anpassung an spezifische Anforderungen und die Akzeptanz bei den beteiligten Akteuren zu sammeln. Nachfolgend wird geklärt, welche technischen Umsetzungswege Kommunen zur Verfügung stehen.

1. Optionen für die technische Implementierung

Für die technische Umsetzung bestehen prinzipiell vier Optionen, die verschiedene Vor- und Nachteile aufweisen.¹⁵ Da der lokale Betrieb von KI-Systemen für die meisten Kommunen derzeit aus den genannten Gründen häufig nicht realisierbar ist, liegt der Fokus im weiteren Verlauf auf den für Kommunalverwaltungen im Regelfall relevanten Umsetzungsvarianten:

- a. Nutzung im Internet öffentlich zugänglicher KI-Systeme
- b. Beschaffung als Software-Dienst
- c. Bereitstellung von KI über Cloud-Plattformen

a. Öffentlich zugängliche KI-Systeme

Bei der ersten Variante greifen Kommunalverwaltungen auf frei verfügbare KI-Anwendungen im Internet zurück. Dieser Weg erfordert keine eigene Infrastruktur, birgt jedoch Risiken hinsichtlich Datenschutz und Anpassbarkeit. Die Nutzung öffentlich zugänglicher KI-Systeme bietet Kommunalverwaltungen einige Vorteile, aber auch wesentliche Nachteile.

Ein klarer Vorteil ist der einfache und kurzfristige Zugang zu KI-Anwendungen, da sie in der Regel direkt über den Web-Browser genutzt werden können. Zudem entstehen keine zusätzlichen Kosten für spezielle KI- oder Cloud-Dienste, was die Einstiegshürde niedrig hält.

Auf der anderen Seite gibt es jedoch auch erhebliche Nachteile. Um ein Mindestmaß an Datenschutz und Datensicherheit herzustellen, ist eine Registrierung mit personenbezogenen Daten wie einer E-Mail-Adresse erforderlich, was den Zugang zwar erleichtert, aber weitere datenschutzrechtliche Fragen aufwirft, wenn die dienstliche E-Mail-Adresse verwendet wird. Die Verarbeitung der eingegebenen Daten in öffentlich zugängliche KI-Systemen ist oft intransparent und es kann sein, dass die Daten von den Anbietern für das Training ihrer Modelle verwendet werden. Da auch nach erfolgter Registrierung nur eingeschränkt individuelle Datenschutzmaßnahmen umgesetzt werden können, bestehen potenzielle Risiken in Bezug auf

¹⁵ Vgl. dazu die Ausführungen zur Methodik in der Einleitung.

die Datensicherheit. Darüber hinaus sind öffentlich zugängliche KI-Systeme in ihrer Funktionalität meist nur eingeschränkt anpassbar, was die Nutzung für spezifische Anforderungen erschwert. Tabelle 1 fasst die Vor- und Nachteile für diese Implementierungsvariante zusammen.

| Nutzung öffentlich zugänglicher KI-Systeme | |
|---|--|
| Vorteile | Nachteile |
| <ul style="list-style-type: none"> ▪ Einfacher und kurzfristiger Zugang zu KI ▪ Keine zusätzlichen KI- oder Cloud-Dienste erforderlich ▪ KI lässt sich einfach über den Web-Browser nutzen | <ul style="list-style-type: none"> ▪ Häufig Registrierung mit E-Mail-Adresse erforderlich ▪ Datenverarbeitung intransparent ▪ Potenziell geringe Datensicherheit ▪ Eingeschränkte Anpassbarkeit ▪ Daten können durch Anbieter für Modelltraining verwendet werden ▪ Keine individuellen Datenschutzmaßnahmen möglich |

Tabelle 1: Vor- und Nachteile der Nutzung öffentlich zugänglicher KI-Systeme.

b. Beschaffung als Software-Dienst

Bei der zweiten Option werden KI-Systeme als Software-Dienst (*Software-as-a-Service, SaaS*) von spezialisierten Anbietern bezogen. Die Anbieter übernehmen Betrieb, Wartung und Updates, während die Kommunen die Dienste flexibel nutzen können. Das vereinfacht die Implementierung, erfordert aber klare vertragliche Regelungen zu Datenschutz und Datensicherheit. Zu den Vorteilen der Variante zählt, dass Anbieter Software-Dienste kurzfristig bereitstellen können und keine Investitionen in eine eigene IT-Infrastruktur erforderlich ist. Zudem sind SaaS-Lösungen einfach skalierbar und können, beispielsweise im Hinblick auf die Anzahl an Nutzern/Lizenzen, je nach Bedarf reduziert oder ausgeweitet werden. Regelmäßige Updates und die schnelle Integration neuer KI-Funktionen sorgen dafür, dass die Systeme aktuell bleiben. Darüber hinaus profitieren Kommunen von technischem Support und Wartung durch die Anbieter, die oft über Spezialkenntnisse und Zertifizierungen verfügen, was potenziell eine höhere Datensicherheit gewährleistet. Dank tarifbasierter Preismodelle wird außerdem die Budgetplanung erleichtert.

Allerdings gibt es auch einige Nachteile, die Kommunen berücksichtigen müssen. Auch als Software-Dienste betriebene KI-Systeme müssen sich in die bestehende IT-Infrastruktur der Kommune einfügen – das betrifft im Regelfall mindestens die Registrierung/Anmeldung von Nutzern sowie die Kompatibilität mit der Systemumgebung bzw. dem Betriebssystem und dem Web-Browser. Beispielsweise könnte es erforderlich sein, dass die Anmeldung über ein zentrales Single-Sign-On-System (SSO) erfolgt, was eine Verbindung zum verwendeten Identifizierungsdienst erfordert, die Kompatibilität des KI-Systems mit dem Dienst voraussetzt und zur Übertragung von Authentifizierungsdaten zwischen der Kommune und dem KI-Anbieter führt.

Während die kurzfristigen Kosten oftmals gering sind, können sich die laufenden Gebühren langfristig summieren und zu einer finanziellen Belastung werden, wenn der Dienst elementarer Bestandteil kommunaler Vorgänge etwa im Bürger-Service oder in digitalen Antragsprozessen wird. Zudem haben Kommunen möglicherweise nur eingeschränkte Kontrolle und

Transparenz über die Datenverarbeitung, insbesondere wenn Daten auf Servern im Ausland gespeichert werden. Um das zu vermeiden, müssen Kommunen Sorgfalt bei der Auswahl des Anbieters und der Vertragsgestaltung an den Tag legen. Die Gestaltung von Verträgen für KI-Systeme kann je nach Anwendungsfall komplex sein, da Aspekte wie Service-Level-Agreements, Datenschutz, Datensicherheit und Compliance individuell geregelt werden müssen.

Darüber hinaus besteht die Gefahr einer Abhängigkeit von einem einzelnen Anbieter, was bei Preisänderungen oder einem Anbieterwechsel problematisch sein könnte. Schließlich bieten SaaS-Lösungen oft nur begrenzte Anpassungsmöglichkeiten, was die Berücksichtigung spezifischer kommunaler Anforderungen erschweren kann. Beispielsweise lässt sich ein für die Öffentlichkeit bestimmter Webseiten-Chatbot nicht ohne weiteres zur Indizierung von Dokumenten zur Optimierung interner Recherchen einsetzen. Tabelle 2 fasst die Vor- und Nachteile für diese Implementierungsvariante zusammen.

| Nutzung von KI-Systemen als Software-Dienst | |
|--|---|
| Vorteile | Nachteile |
| <ul style="list-style-type: none"> ▪ Kurzfristig bereitstellbar ▪ Keine Investitionen in IT-Infrastruktur erforderlich ▪ Einfach skalierbar und reduzierbar ▪ Regelmäßige Updates ▪ Schnelle Integration neuer Funktionen ▪ Technischer Support und Wartung ▪ Potenziell höhere Sicherheit durch Anbieterexpertise ▪ Budgetplanung durch Tarif-basierte Preismodelle | <ul style="list-style-type: none"> ▪ Lösung muss sich in die IT-Infrastruktur der Kommune einfügen ▪ Möglicherweise hohe langfristige Kosten ▪ Möglicherweise eingeschränkte Kontrolle und Transparenz über Datenverarbeitung ▪ Je nach Anwendungsfall komplexe Vertragsgestaltung (Service-Level-Agreement, Datenschutz, Datensicherheit, Compliance) ▪ Ggf. Datenverarbeitung im Ausland ▪ Ggf. Abhängigkeit von einem Anbieter ▪ Geringe Anpassungsmöglichkeiten an spezifische kommunale Anforderungen |

Tabelle 2: Vor- und Nachteile der Nutzung von KI-Systemen als Software-Dienst.

c. Bereitstellung von KI über Cloud-Plattformen

KI-Anwendungen werden bei der dritten Variante über Cloud-Dienste bereitgestellt, die von externen Anbietern betrieben werden.

Diese Umsetzungsoption bietet Kommunen eine flexible Möglichkeit, auf fortschrittliche KI-Technologie zuzugreifen, ohne dazu in eigene IT-Infrastruktur investieren zu müssen. Ein wesentlicher Vorteil ist der Zugang zu unterschiedlichen KI-Modellen. Zudem lassen sich Cloud-basierte KI-Lösungen individuell konfigurieren, wobei oftmals vorgefertigte Tools und Frameworks zur Verfügung stehen, die die Entwicklung und Anpassung erleichtern und zum Teil keine Programmierkenntnisse erfordern (*No-code/Low-code*).

Viele Cloud-Anbieter weisen marktübliche Zertifizierungen auf und bieten eine hohe Transparenz über die Datenverarbeitung und den Datenschutz, was die Einhaltung rechtlicher Vorgaben wie der DS-GVO erleichtert. Außerdem werden Cloud-Dienste im Regelfall über einen eigenen Mandanten implementiert. Dabei handelt es sich um einen eigenständig durch die Kommune administrierbaren Bereich mit logischer Datentrennung, der als dedizierter Bereich innerhalb der Cloud-Plattform des Anbieters betrieben wird.¹⁶ Dies ermöglicht Kommunen eine

¹⁶ StMFH Bayern, KI-Leitfaden, 2025, S. 19.

umfassende Kontrolle über die Datenverarbeitung und Datensicherheit. Die Nutzung eines eigenen Mandanten ist beispielsweise dann von Bedeutung, wenn Kommunen Daten und Dokumente in der Cloud speichern und indizieren möchten, um sie mittels KI durchsuchbar zu machen. Darüber hinaus stellt die Datentrennung sicher, dass möglicherweise archivierte Chatverläufe für den Cloud-Anbieter unzugänglich bleiben.

Ein weiterer Vorteil ist die einfache Skalierbarkeit der Dienste, die es ermöglicht, die Nutzung flexibel an den tatsächlichen Bedarf anzupassen. Das sorgt insbesondere bei nutzungsbasierten Abrechnungsmodellen für eine bessere Kostenkontrolle. Regelmäßige Updates und technischer Support gewährleisten, dass die Systeme auf dem neuesten Stand sind und bei Problemen Unterstützung angefragt werden kann. Darüber hinaus bieten viele Cloud-Plattformen Schnittstellen, die eine Interoperabilität und Integration mit anderen Systemen ermöglichen.

Trotz der verschiedenen Vorteile gibt es auch einige Herausforderungen, die berücksichtigt werden müssen. Der Aufwand für das Deployment und den Betrieb der Cloud-Umgebung sowie der KI-Dienste kann erheblich sein, insbesondere wenn die Plattform nicht nahtlos in die bestehende IT-Infrastruktur integriert werden kann. Das kann beispielsweise der Fall sein, wenn die Kommune die grundsätzliche Entscheidung gegen die Nutzung von Cloud-Diensten getroffen hat, aber zum Zweck der KI-Nutzung eine Ausnahme macht. In dem Fall können die Cloud-Plattform und das lokale Netzwerk als parallele Strukturen bestehen. Diese Herausforderung ist weniger stark ausgeprägt, wenn die Kommune auch in anderen Bereichen auf Cloud-Dienste zurückgreift – etwa auf dem Gebiet der Bürokommunikation, für Web-Konferenzen, und als Werkzeug für kollaboratives Arbeiten.

Für die Einrichtung und Konfiguration von KI über Cloud-Plattformen sind zudem spezielle IT-Kenntnisse und ein grundlegendes Verständnis der Technologien erforderlich, um die Dienste effektiv nutzen und verwalten zu können. Die Vertragsgestaltung mit Cloud-Anbietern kann komplex sein, da Aspekte wie Service-Level-Agreements, Datenschutz, Datensicherheit und Compliance individuell geregelt werden müssen. Ein weiterer Nachteil ist die potenzielle Abhängigkeit von einem Anbieter, was problematisch werden kann, wenn dieser die Preise erhöht, den Dienst einstellt oder die Vertragsbedingungen ändert.

Die Nutzung von Cloud-Diensten wird in vielen Kommunen skeptisch betrachtet, insbesondere wenn kommunale Daten in der Cloud gespeichert werden sollen. Selbst wenn sich die Nutzung von Cloud-Diensten nur auf die Verarbeitung von Prompts beschränkt, sehen viele Kommunen ein Problem, vor allem wenn auf ausländische Cloud-Anbieter zurückgegriffen wird. Hier ist anzumerken, dass KI-Modelle aufgrund der erforderlichen Rechenleistung auf absehbare Zeit meistens als Cloud-Dienst zur Verfügung stehen werden. Kommunen stehen daher vor der Wahl: Sie können entweder selbst mehr Verantwortung übernehmen, was eine höhere Kontrolle und Transparenz über die Datenverarbeitung und Datensicherheit ermöglicht, oder sie können KI-Systeme als Software-Dienste beschaffen, wodurch sie Verantwortung an den Dienstleister übertragen, jedoch möglicherweise Einschränkungen bei der Transparenz und Kontrolle über die Datenverarbeitung und Datenhaltung in Kauf nehmen müssen.

Insgesamt bietet die Umsetzung über eine Cloud-Plattform viele Vorteile, erfordert jedoch eine sorgfältige Planung, klare vertragliche Regelungen und technisches Know-how, um die Risiken zu minimieren und die Vorteile optimal zu nutzen. Die Entscheidung für oder gegen eine Cloud-Lösung sollte dabei stets unter Berücksichtigung der spezifischen Anforderungen und Rahmenbedingungen der jeweiligen Kommune getroffen werden. Tabelle 3 fasst die Vor- und Nachteile für diese Implementierungsvariante zusammen.

| Bereitstellung von KI über Cloud-Plattformen | |
|---|---|
| Vorteile | Nachteile |
| <ul style="list-style-type: none"> ▪ Zugang zu unterschiedlichen KI-Modellen ▪ KI-Lösungen lassen sich individuell konfigurieren ▪ Oftmals vorgefertigte Tools und Frameworks verwendbar ▪ Höhere Transparenz über Datenverarbeitung und Datenschutz ▪ Keine Investitionen in IT-Infrastruktur erforderlich ▪ Einfach skalierbar und reduzierbar ▪ Kostenkontrolle ▪ Regelmäßige Updates und technischer Support ▪ Interoperabilität und Integration über Schnittstellen | <ul style="list-style-type: none"> ▪ Aufwand für Deployment und Betrieb der Cloud-Umgebung und der KI-Dienste ▪ Spezielle IT-Kenntnisse und Verständnis von KI-Technologien erforderlich ▪ Komplexe Vertragsgestaltung (Service-Level-Agreement, Datenschutz, Datensicherheit, Compliance) ▪ Ggf. Abhängigkeit von einem Anbieter |

Tabelle 3: Vor- und Nachteile der Bereitstellung von KI über Cloud-Plattformen.

2. Zwischenfazit

Kommunen sollten den Einstieg in den Einsatz von KI-Technologien mit Pilotprojekten beginnen, um erste Erfahrungen zu sammeln und die Akzeptanz zu fördern. Die Wahl der technischen Implementierungsvariante hängt dabei von der Größe der Kommune, den verfügbaren personellen und finanziellen Ressourcen, dem vorhandenen IT-Know-how und dem allgemeinen Stand der Digitalisierung ab.

Die verschiedenen Möglichkeiten für die technische Umsetzung weisen unterschiedliche Vor- und Nachteile auf, die Kommunen sorgfältig abwägen sollten. Beispielsweise bieten öffentlich zugängliche KI-Systeme zwar niedrige Einstiegshürden, bringen jedoch Risiken in Bezug auf Datenschutz, Datensicherheit und Anpassbarkeit mit sich. Software-Dienste zeichnen sich durch Flexibilität und Serviceleistungen aus, können jedoch langfristig hohe Kosten und Abhängigkeiten verursachen. Cloud-Plattformen ermöglichen eine hohe Flexibilität und Skalierbarkeit, erfordern jedoch technisches Know-how und eine sorgfältige Vertragsgestaltung.

In allen Fällen ist der Schutz sensibler Daten ein zentraler Aspekt, den Kommunen in der Abwägung – insbesondere bei der Nutzung externer Dienste – berücksichtigen sollten. Neben den kurzfristigen Vorteilen einer Variante sollten Kommunen auch die potenziellen langfristigen finanziellen Belastungen durch laufende Gebühren oder Abhängigkeiten von Anbietern berücksichtigen. Die Wahl der KI-Lösung sollte stets auf die spezifischen Anforderungen und Ziele der jeweiligen Kommune abgestimmt sein, um den größtmöglichen Nutzen zu erzielen.

V. IT-Sicherheit

Bislang konnte geklärt werden, welche technischen Umsetzungsvarianten für die Nutzung von KI bestehen. Fraglich ist, welche Anforderungen an die Sicherheit von kommunalen IT-Systemen bestehen, wenn KI-Systeme eingesetzt werden.

1. BSI-Schichtenmodell bei kommunalen KI-Projekten

KI-Systeme sind im Allgemeinen wie IT-Systeme zu betrachten und unterliegen denselben Vorgaben für die IT-Sicherheit.¹⁷

Ein zentraler Baustein für die Prüfung der IT-Sicherheit in Kommunen ist der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI). Er bietet Methoden, Anleitungen und Empfehlungen zum Schutz kommunaler Daten, Systeme und Informationen und sieht entsprechende technische, organisatorische und infrastrukturelle Maßnahmen vor. Der IT-Grundschutz des BSI stellt auch bei kommunalen KI-Projekten eine Basisgröße zur Prüfung der IT-Sicherheitsanforderungen dar.

Referenzen für übergreifende Strukturen der kommunalen IT-Sicherheit sind die BSI-Standards über das Informationssicherheits-Management (ISMS). Sie bilden im Schichtmodell des IT-Grundschutz-Kompendiums die oberste Schicht, über einzelnen Prozess- und Systembausteinen und dem Baustein für Detektion und Reaktion.¹⁸ Beim ISMS geht es um die Planungs-, Lenkungs- und Kontrollaufgaben, die erforderlich sind, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen.¹⁹ Das ISMS betrifft den IT-Verbund einer Kommune insgesamt und sollte unabhängig davon aufgebaut werden, ob KI-Projekte durchgeführt werden oder nicht.

Für welche Prozess- und Systembausteine die Kommune bei KI-Projekten die Verantwortung trägt, hängt von der jeweiligen Implementierungsvariante ab. Das betrifft im Regelfall die Beschaffung als Software-Dienst und die Bereitstellung von KI-Diensten über Cloud-Plattformen (dazu oben unter IV.1). Dabei gilt, dass die Kommune umso mehr eigene Verantwortung trägt, je mehr Aufgaben sie zur Bereitstellung einer IT-Leistung selbst erfüllt (Tabelle 4).

Kauft eine Kommune eine KI-Anwendung als Software-Dienst ein, muss sie sich grundsätzlich nur um die verarbeiteten Informationen und Daten und die verwendeten Endgeräte, Accounts und Identitäten kümmern (Tabelle 4).

Bei der Nutzung von KI-Diensten über Cloud-Plattformen kann die Verteilung der Verantwortung über die herkömmlichen Ansätze hinausgehen. Häufig wird der Anbieter für die Bereitstellung und Sicherung der zugrunde liegenden Infrastruktur, der KI-Modelle und der Plattform verantwortlich sein, während die Kommune die Verantwortung für den konkreten Einsatz der KI in ihrem Zuständigkeitsbereich trägt.²⁰ Dazu gehören der Schutz sensibler kommunaler Daten, die sichere Gestaltung und Verwaltung von Eingaben, die Minimierung von Risiken wie Manipulationen sowie die Einhaltung gesetzlicher, regulatorischer und interner Vorgaben.²¹

¹⁷ StMFH Bayern, KI-Leitfaden, 2025, S. 31.

¹⁸ BSI, Schichtenmodell, 2025.

¹⁹ BSI, ISMS, 2023, S. 1

²⁰ Microsoft, Shared responsibility, 2025.

²¹ Ebd.

| Verortung | Verantwortung für | SaaS | PaaS | IaaS | On-prem |
|--|-------------------------------------|------|------|------|---------|
| Verantwortung verbleibt immer bei der Kommune | Informationen und Daten | K | K | K | K |
| | Endgeräte | K | K | K | K |
| | Accounts und Identitäten | K | K | K | K |
| Verteilung der Verantwortung kann variieren | Identitäts- und Ordnerinfrastruktur | G | G | K | K |
| | Anwendungen | A | G | K | K |
| | Netzwerk | A | G | K | K |
| | Betriebssystem | A | A | K | K |
| Verantwortung geht auf den Cloud-Anbieter über | Physische Hosts | A | A | A | K |
| | Physisches Netzwerk | A | A | A | K |
| | Physische Datenzentren | A | A | A | K |

Tabelle 4: Allgemeine Verteilung der Verantwortung in Abhängigkeit der technischen Implementierung (Microsoft, Geteilte Zuständigkeit 2025). Abkürzungen: SaaS = Software-as-a-Service, PaaS = Platform-as-a-Service, IaaS = Infrastructure-as-a-Service, On-prem = On-premise, K = Kunde/Kommune, G = geteilte Verantwortung, A = Anbieter. Tabelle in Anlehnung an: Microsoft, Shared responsibility, 2025.

Festzuhalten ist, dass KI-Systeme in Kommunen grundsätzlich wie IT-Systeme behandelt werden sollten und denselben IT-Sicherheitsvorgaben unterliegen. Der IT-Grundschutz des BSI bildet eine Basisgröße auch für KI-Projekte und wird durch ein ISMS ergänzt, das die übergreifenden Strukturen der Informationssicherheit regelt. Die Verantwortung der Kommune bei der Nutzung von KI-Diensten hängt von der Implementierungsvariante ab und nimmt mit dem Grad der Eigenleistung zu, insbesondere im Hinblick auf den Schutz sensibler Daten und die Einhaltung regulatorischer Vorgaben.

2. Spezielles BSI-Material zum Einsatz von KI

Ergänzend zu den Dokumentationen des IT-Grundschutzes hat das BSI Material betreffend die Nutzung von KI – insbesondere generativer KI – veröffentlicht. Damit möchte es ein grundlegendes Sicherheitsbewusstsein für KI-Modelle schaffen und ihren sicheren Einsatz fördern, indem es dessen Chancen und Risiken analysiert und Maßnahmen vorschlägt.²²

Das BSI unterteilt die Risiken von generativer KI in drei Kategorien: Risiken bei ordnungsgemäßer Nutzung, Risiken durch missbräuchliche Nutzung und Risiken durch gezielte Angriffe.²³ Die durch das BSI identifizierten Chancen und Risiken werden im vorliegenden Arbeitspapier nicht einzeln dargestellt. Der Fokus liegt vielmehr auf den vom BSI vorgeschlagenen Maßnahmen, die Kommunen in eigenen KI-Projekten prüfen können, um den Risiken zu begegnen.

a. Maßnahmen zur Risikominderung bei generativer KI

Nachfolgend werden die vom BSI genannten Risikominderungsmaßnahmen aufgelistet.²⁴

Da es in kommunalen KI-Projekten meistens um den Einsatz von großen Sprachmodellen geht, werden spezielle Informationen mit Bezug zu Bild- und Videogeneratoren nicht berücksichtigt.

²² BSI, Generative KI-Modelle, 2025, S. 5.

²³ Ebd.

²⁴ Nachfolgend zusammengefasst aus: BSI, Generative KI-Modelle, 2025, S. 36-51.

Einige Maßnahmen beziehen sich außerdem speziell auf den Fall, dass eine Behörde eigene KI-Anwendungen entwickelt. Auch diese Maßnahmen werden in der folgenden Liste nicht aufgeführt. Der Fokus liegt hier auf Maßnahmen, in denen eine Behörde als Betreiber oder Nutzer fungiert.

Risikominderungsmaßnahmen des BSI beim Einsatz von KI (insb. LLM)

1) Auswahl des Modells

Kommunen können Kriterien für die Auswahl generativer KI-Modelle und ihrer Anbieter entwickeln, um ihre Funktionalität, Sicherheit, die Einhaltung rechtlicher Anforderungen und die möglichen Risiken zu bewerten.

2) Sicherstellen der Erklärbarkeit

Kommunen können auf erklärbar – das heißt für Menschen verständliche – KI-Modelle setzen, um ihre Funktionsweise und Ausgaben für die beteiligten Akteure nachvollziehbar zu machen.

3) Detektion KI-generierter Inhalte

Kommunen können technische Verfahren einsetzen, um KI-generierte Inhalte zu erkennen und so Missbrauch zu verhindern.

4) Steigerung der Robustheit

Kommunen können beispielsweise durch adversariales Training (Training mit bewusst manipulierten Daten) die Robustheit von Modellen erhöhen und unerwünschte Reaktionen minimieren.

5) Durchführung umfassender Tests

Kommunen können generative KI-Modelle regelmäßig testen, um Schwachstellen und unerwünschte Ausgaben zu identifizieren und zu beheben.

6) Validierung, Sanitarisierung und Formatierung der Eingaben

Kommunen können das KI-System so anpassen, dass Eingaben vor der Übergabe an ein KI-Modell auf manipulative oder böswillige Absicht geprüft werden, um die Erstellung von schädlichen oder böswilligen Inhalten zu verhindern.

7) Validierung und Sanitarisierung der Ausgaben

Kommunen können Ausgaben auf schädliche oder sensible Inhalte prüfen und bei Bedarf filtern oder mit Warnhinweisen versehen.

8) Retrieval-Augmented Generation (RAG)

Kommunen können RAG nutzen, um Modelle mit aktuellen und relevanten Informationen aus eigenen Wissensdatenbanken anzureichern.

9) Einschränkung des Zugriffs auf das Modell

Kommunen können den Zugriff auf Modelle durch Nutzerrechte und Nutzungsbeschränkungen auf das notwendige Minimum reduzieren. Außerdem können sie die Anzahl der Eingaben absolut oder innerhalb einer bestimmten Zeitspanne begrenzen, um automatisierte Anfragen oder das iterative Anpassen von Eingaben zur Umgehung von Filtermechanismen zu erschweren.

10) Sensibilisierung und Aufklärung über Nutzungsrisiken

Kommunen können Nutzer über die Risiken generativer KI-Modelle aufklären und klare Richtlinien für deren Einsatz bereitstellen. Die Nutzer können dadurch in die Lage versetzt werden, Ausgaben des Modells kritisch zu hinterfragen, deren Inhalte ggf. anzupassen und ihre Weiterverwendung eventuell einzuschränken

11) Einschränkung der Rechte LLM-basierter Anwendungen

Kommunen können die Rechte von LLM-basierten Anwendungen auf das notwendige Minimum beschränken und kritische Aktionen durch Nutzer bestätigen lassen. Dazu können sie Vertrauensgrenzen zwischen dem Modell, der auf ihm basierenden Anwendung, externen Ressourcen und erweiterten Funktionalitäten festlegen.

12) Sparsamer Umgang mit sensiblen Daten

Kommunen können die Eingabe und Verarbeitung sensibler Daten minimieren und auf Anonymisierung und Filterung setzen. Als Betreiber sollten Kommunen umsichtig mit Daten aus Nutzerprofilen einerseits und aus getätigten Eingaben und generierten Ausgaben andererseits umgehen. Sie können untersuchen, ob eine Filterung und/oder Anonymisierung der Ein- und Ausgaben, die zum Training verwendet werden, zum Schutz der Nutzer erforderlich ist und technisch umgesetzt werden kann.

13) Logging und Monitoring

Kommunen können durch automatisiertes Logging und Monitoring die Nutzung von der KI-Modelle überwachen, um unerwünschtes Verhalten frühzeitig zu erkennen.

14) Prüfung und Nachbearbeitung der Ausgaben

Kommunen können kritische Ausgaben vor der Weiterverwendung prüfen, mit anderen Quellen abgleichen und bei Bedarf manuell anpassen. Das gilt insbesondere, wenn generierte Ausgaben für die Öffentlichkeit bestimmt sind.

Festzuhalten ist, dass das BSI umfassende Maßnahmen zur sicheren Nutzung generativer KI-Modelle empfiehlt. Sie zielen darauf ab, Risiken wie Missbrauch, unerwünschte Ausgaben oder Angriffe zu minimieren und gleichzeitig die Funktionalität, Sicherheit und Transparenz der verwendeten KI-Modelle zu gewährleisten.

Kommunen können durch die gezielte Auswahl von Modellen, die Sicherstellung ihrer Erklärbarkeit, technische Prüfungen, Einschränkung von Zugriffsrechten und die Sensibilisierung der Nutzer Risiken adressieren und den verantwortungsvollen Einsatz von KI fördern.

b. BSI-Kriterienkatalog für generative KI

Das BSI hat einen Katalog veröffentlicht, der Kriterien definiert, die aus Sicht des BSI bei der Integration extern bereitgestellter generativer KI-Modelle in eigene Anwendungen in der Bundesverwaltung erfüllt werden sollten, um ein Mindestsicherheitsniveau zu erreichen.²⁵

Der Kriterienkatalog beschränkt sich auf die Regelung der Integration extern bereitgestellter generativer KI-Modelle in eigene Anwendungen. Regelungen, die die reine Nutzung solcher Dienste (ohne eine Integration) betreffen, können aber teilweise aus dem Katalog abgeleitet

²⁵ BSI, Kriterienkatalog, 2025, S. 4.

werden.²⁶ Dadurch stellt der Kriterienkatalog eine hilfreiche Orientierung für Kommunen dar, die generative KI nutzen möchten.

Die wesentlichen Inhalte des Kriterienkatalogs werden nachfolgend zusammenfassend dargestellt.²⁷

Im Rahmen einer globalen KI-Governance empfiehlt das BSI zunächst, grundlegende Maßnahmen zu etablieren, die unabhängig vom spezifischen Anwendungsfall gelten. Dazu gehören die Koordination und Verwaltung aller KI-Aktivitäten durch eine verantwortliche Person, die Erstellung einer Anwendungsübersicht, die Definition von Nutzungsbedingungen, ein Schwachstellenmanagement sowie Schulungen für Endnutzer.

Für die Integration von KI-Modellen empfiehlt der Kriterienkatalog eine strukturierte Vorgehensweise in mehreren Phasen. In der Planungsphase sollte der Anwendungsfall klar definiert und auf dieser Grundlage Auswahlkriterien für das KI-Modell festgelegt werden, die spezifische Risiken berücksichtigen. Zudem ist die Vertrauenswürdigkeit des Anbieters zu bewerten.

In der Beschaffungsphase wird das KI-Modell anhand der definierten Kriterien beurteilt. Dabei ist sicherzustellen, dass das Modell aus vertrauenswürdigen Quellen stammt und die geltenden Cloud-Nutzungsstandards eingehalten werden. Falls erforderlich, können in der anschließenden Anpassungsphase Modifikationen am KI-Modell vorgenommen werden, beispielsweise die zentrale Verwaltung von System-Prompts ohne sensible Daten.

Die Integrationsphase umfasst die Einbindung der Anwendung in das bestehende Informationssicherheitsmanagementsystem (ISMS). Hierbei empfiehlt das BSI, eine Gefahrenmodellierung durchzuführen und Sicherheitsmaßnahmen zu ergreifen, um die Integration abzusichern. Während der Einsatzphase liegt der Fokus auf der Verhinderung missbräuchlicher Nutzung und der Beschränkung des Zugriffs auf das notwendige Minimum. In der Beendigungsphase ist schließlich sicherzustellen, dass alle sensiblen Daten geordnet aus der Anwendung entfernt werden, sobald die Nutzung endet.

Festzuhalten ist, dass der Kriterienkatalog des BSI eine wertvolle Orientierung bietet, um in kommunalen KI-Projekten grundlegende Sicherheitsanforderungen zu berücksichtigen und die Integration von KI-Modellen sicher zu gestalten.

3. Zwischenfazit

Kommunen können für KI-Projekte im Hinblick auf die IT-Sicherheit die allgemeinen Vorgaben des BSI, insbesondere über den IT-Grundschutz und das Informationssicherheitsmanagementsystem, als Grundlage heranziehen. Sie bieten bewährte Methoden und Standards, um die Sicherheit von IT-Systemen – einschließlich KI-Anwendungen – zu gewährleisten.

Ergänzend hat das BSI Material mit Maßnahmenvorschlägen veröffentlicht, die sich insbesondere auf die sichere Nutzung generativer KI-Modelle konzentrieren. Dazu zählen unter anderem Empfehlungen zur Auswahl geeigneter Modelle, zur Minimierung von Risiken wie Missbrauch oder Manipulation sowie zur Sicherstellung von Transparenz und Erklärbarkeit.

²⁶ Ebd., S. 4-5.

²⁷ Hier und im Folgenden: BSI, Kriterienkatalog, 2025, S. 8-13. Die einzelnen Maßnahmen für jede Phase sind im Anhang zum Arbeitspapier aufgeführt.

Der Kriterienkatalog des BSI zum Einsatz generativer KI bietet darüber hinaus eine strukturierte Orientierung für die Integration externer KI-Modelle in kommunale Anwendungen. Er definiert konkrete Maßnahmen für die verschiedenen Projektphasen von der Planung über die Beschaffung bis hin zur Nutzung und Beendigung.

VI. Rechtliche und organisatorische Aspekte

Fest steht, dass ein zentraler Erfolgsfaktor für die Nutzung von KI in Kommunen darin besteht, erste Erfahrungen mit der Implementierung und Anwendung zu sammeln, um die Potenziale und Herausforderungen von KI besser zu verstehen. Gleichzeitig ist es essenziell, Strukturen für den systematischen und langfristigen Einsatz von KI zu schaffen. Die gesamte Menge an internen Strukturen und Prozessen, die Einsatz von KI in einer Kommune regeln und fördern, wird als „KI-Governance“ bezeichnet. Sie umfasst vor dem Hintergrund der rechtlichen Vorgaben die organisatorischen und technischen Rahmenbedingungen, die erforderlich sind, um den Einsatz von KI in kommunalen Strukturen zu gestalten.

Nachfolgend werden zunächst die beim Einsatz von KI zu beachtenden rechtlichen Vorgaben geklärt. Der Schwerpunkt liegt dabei auf den Anforderungen der EU KI-Verordnung und des Datenschutzrechts (vgl. die Überlegungen zur Methodik in der Einleitung). Darüber hinaus wird summarisch auf die Vorgaben über die Mitwirkung und Mitbestimmung der Personalvertretung eingegangen.

Zuletzt geht es um die Frage, welche Inhalte Kommunen in internen Vorgaben wie Dienstweisungen und Dienstvereinbarungen vorsehen können, um die Nutzung von KI in ihrer Organisation zu regeln.

1. Rechtlicher Rahmen, insb. EU KI-VO und Datenschutzrecht

Die EU KI-Verordnung, das Datenschutzrecht und die Mitbestimmungs- und Mitwirkungsrechte der Personalvertretung bilden einen wesentlichen Teil der rechtlichen Rahmenbedingungen für den Einsatz von KI-Systemen in Kommunen ab.

Die KI-Verordnung schafft einen einheitlichen Rechtsrahmen für die Entwicklung und Nutzung von KI in der Union, während das Datenschutzrecht, insbesondere die Datenschutz-Grundverordnung (DS-GVO), essenziell für den Schutz personenbezogener Daten ist, die bei der Nutzung von KI verarbeitet werden können. Gleichzeitig sind die Mitbestimmungs- und Mitwirkungsrechte der Personalvertretung zu beachten, da der Einsatz von KI-Systemen Auswirkungen auf die Arbeitsbedingungen und die Rechte der Beschäftigten haben kann.

a. Anforderungen der EU KI-VO an die kommunale KI-Nutzung

Die Verordnung (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz ist am 1. August 2024 in Kraft getreten und gilt auch für Kommunalverwaltungen. Fraglich ist, welche Anforderungen der Verordnung Kommunen bei der Nutzung von KI zu beachten haben.

Ein zentraler Bestandteil des Rechtsaktes ist der risikobasierte Ansatz, der die Nutzung von KI-Systemen nach ihrem potenziellen Risiko für die Gesellschaft, die Sicherheit oder die Grundrechte unterschiedlich reguliert. Bestimmte KI-Praktiken, die als besonders gefährlich oder ethisch bedenklich eingestuft werden, sind verboten. Für sogenannte „Hochrisiko-KI“ gel-

ten besonders strenge Vorgaben, die unter anderem Anforderungen an Transparenz, Nachvollziehbarkeit und Sicherheit umfassen. Darüber hinaus werden sowohl Anbieter als auch Betreiber von KI-Systemen in die Pflicht genommen, spezifische Vorgaben einzuhalten, um einen verantwortungsvollen und sicheren Einsatz von KI zu gewährleisten.

Gemäß Art. 3 Nr. 1 der Verordnung wird ein „KI-System“ durch mehrere Merkmale definiert. Es handelt sich dabei um ein maschinengestütztes System, das für einen autonomen Betrieb ausgelegt ist. Ein solches System kann anpassungsfähig sein, das heißt, in der Lage sein, sich auf Grundlage von neuen Daten oder Beobachtungen weiterzuentwickeln. KI-Systeme reagieren gemäß der Legaldefinition auf Eingaben, um explizite oder implizite Ziele zu erreichen, und erzeugen dazu Ausgaben wie Vorhersagen, Empfehlungen oder Entscheidungen. Diese Ausgaben können sowohl physische als auch virtuelle Umgebungen beeinflussen.

Vereinfacht ausgedrückt ist ein KI-System die gesamte „Maschinerie“, die benötigt wird, um ein KI-Modell in der Praxis nutzen zu können.²⁸ Es besteht nicht nur aus dem KI-Modell selbst, sondern auch aus allem, was drumherum nötig ist, wie zum Beispiel Benutzeroberflächen oder Kommunikationsprotokollen.²⁹

Ein „KI-Modell“ im Sinne der Verordnung ist das mathematische Herzstück oder „Gehirn“ eines KI-Systems.³⁰ Es handelt sich dabei beispielsweise um ein vortrainiertes neuronales Netz, das die Grundlage für die Verarbeitung von Daten und die Erzeugung von Ergebnissen bildet. Solche Modelle sind oft vielseitig einsetzbar und können für ein breites Spektrum an Aufgaben genutzt werden. In der Verordnung wird in Art. 3 Nr. 63 ein „KI-Modell mit allgemeinem Verwendungszweck“ definiert als ein KI-Modell, das eine erhebliche allgemeine Verwendbarkeit aufweist und in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann. Obwohl die Verordnung den allgemeinen Begriff „KI-Modell“ nicht legaldefiniert, lässt sich festhalten, dass es um den Kernmechanismus geht, der die Funktionalität eines KI-Systems ermöglicht.

Die KI-Verordnung sieht vier Risikostufen vor:³¹

- *Unannehmbares Risiko (Verboten)*: KI-Systeme, die ein klares Sicherheitsrisiko darstellen oder die Grundrechte der Bürger in inakzeptabler Weise verletzen, sind grundsätzlich verboten.
- *Hohes Risiko (Streng reguliert)*: Diese KI-Systeme sind nicht verboten, unterliegen aber strengen Auflagen, da sie ein erhebliches Risiko für die Gesundheit, Sicherheit oder die Grundrechte darstellen.
- *Begrenztes Risiko (Transparenzpflichten)*: Für diese Systeme bestehen keine strengen Anforderungen, aber es gibt Transparenzpflichten, damit die Nutzer informierte Entscheidungen treffen können. Der Nutzer muss wissen, dass er mit einer KI interagiert.
- *Minimales Risiko (Weitgehend unreguliert)*: Die Mehrheit der derzeit verwendeten KI-Systeme fällt in diese Kategorie. Sie stellen keine oder nur sehr geringe Risiken dar und sind von den speziellen Vorschriften weitgehend ausgenommen.

²⁸ KGSt, FAQ AI Act, 2025, S. 6.

²⁹ Ebd.

³⁰ Ebd.

³¹ Zusammenfassend: TÜV Rheinland, Klassifikation von KI, 2025.

Kommunalverwaltungen können im Sinne der KI-Verordnung sowohl „Betreiberin“ als auch „Anbieterin“ von KI-Systemen sein.³² Die Rolle der Kommune hängt dabei von der konkreten Nutzung und Bereitstellung des jeweiligen KI-Systems ab.

Ein „Anbieter“ im Sinne der Verordnung (Art. 3 Nr. 3) ist eine Organisation, die ein KI-System entweder selbst entwickelt oder entwickeln lässt. Darüber hinaus gilt eine Organisation als Anbieter, wenn sie ein KI-System unter ihrem eigenen Namen in Verkehr bringt oder es unter ihrem eigenen Namen – entgeltlich oder unentgeltlich – in Betrieb nimmt.

In vielen Fällen wird die Kommune als sogenannter „nachgelagerter Anbieter“ auftreten, wenn sie KI-Modelle oder -Systeme, die von externen Anbietern bereitgestellt werden, integriert und sie unter ihrem eigenen Namen einsetzt.³³ Das ist beispielsweise der Fall, wenn eine Kommune ein Customizing für einen KI-Chatbot betreibt, selbst wenn dieser auf der Basis allgemein zugänglicher KI-Modelle beruht. Allein die Vergabe eines Namens für einen Chatbot, der zum Beispiel als Kommunikation zwischen Verwaltung und Bürgern eingesetzt wird, kann dazu führen, dass die Kommune die Rolle der Anbieterin einnimmt. Als Anbieterin eines KI-Systems hat die Kommunalverwaltung bei Systemen mit begrenztem oder minimalem Risiko gemäß der EU KI-Verordnung verschiedene Pflichten. Dazu gehört die haftungsrechtliche Hauptverantwortung für das KI-System. Außerdem muss sie eine detaillierte technische Dokumentation erstellen, die das System und seine Funktionsweise beschreibt.³⁴

Anbieter sind zudem verpflichtet, ein Verständnis für das Verhalten des Modells, mögliche Voreingenommenheiten und die verwendeten Trainingsdaten zu haben.³⁵ Sie haben auch Transparenz- und Kennzeichnungspflichten zu erfüllen, damit Nutzer wissen, wenn sie mit einer KI interagieren, und KI-generierte Inhalte als solche erkennbar sind.

Eine Kommunalverwaltung kann im Sinne der Verordnung auch „Betreiberin“ eines KI-Systems sein. Nach Art. 3 Nr. 4 KI-VO gilt als Betreiber, wer ein bereits entwickeltes KI-System in eigener Verantwortung verwendet. Tätigkeiten im persönlichen und nicht-beruflichen Bereich sind dabei ausgenommen.

In der Praxis wird die Kommune häufig die Rolle der Betreiberin übernehmen. Beispiele hierfür sind interne Chatbots oder KI-Funktionen, die in bestehende IT-Anwendungen oder Fachverfahren integriert sind. Als Betreiberin eines KI-Systems hat die Kommunalverwaltung verschiedene Pflichten zu erfüllen. Zu den wesentlichen Anforderungen gehören auch hier Transparenz- und Kennzeichnungspflichten: Nutzer müssen darüber informiert werden, dass sie mit einem KI-System interagieren, und KI-generierte Inhalte müssen klar als solche erkennbar sein.³⁶ Dies gilt insbesondere für Anwendungen, die direkt mit der Öffentlichkeit kommunizieren.³⁷

Darüber hinaus gibt es spezielle Regelungen, die in Art. 50 der Verordnung festgelegt sind. Sie betreffen unter anderem Emotionserkennungssysteme, die Verarbeitung von Deepfakes

³² KGSt, FAQ AI Act, 2025, S. 9.

³³ Hier und im Folgenden: Ebd., S. 9, 10.

³⁴ Insgesamt für den Absatz: Ebd., S. 9, 10.

³⁵ KGSt, FAQ AI Act, 2025, S. 9, 10.

³⁶ Ebd., S. 10, 11.

³⁷ Ebd.

sowie Chatbot-Ausgaben, die an die Öffentlichkeit gerichtet sind. Für solche Anwendungen gelten zusätzliche Anforderungen, um Missbrauch und Irreführung zu vermeiden.

Eine weitere Pflicht betrifft die Sicherstellung von KI-Kompetenz innerhalb der Organisation. Art. 4 der Verordnung verlangt, dass Anbieter und Betreiber ein „ausreichendes Maß an KI-Kompetenz“ bei den mit dem Betrieb und der Nutzung von KI-Systemen befassten Personen gewährleisten. Mitarbeiter, die mit KI-Systemen arbeiten, müssen ihre grundlegende Funktionsweise im Kontext des jeweiligen Anwendungsfalls verstehen. Sie sollten außerdem mögliche Fehlerquellen, Voreingenommenheiten sowie ihre eigenen Rechte und Pflichten im Umgang mit der Technologie kennen.³⁸ Dies erfordert entsprechende Schulungen und Weiterbildungen, um die sichere und effektive Nutzung von KI-Systemen zu gewährleisten.

Zusammenfassend lässt sich für die Vorgaben der europäischen KI-Verordnung festhalten:

- Kommunen müssen KI-Systeme entsprechend ihrer Risikostufe bewerten und die jeweiligen Vorgaben einhalten. Sie tragen die Verantwortung für eingesetzte KI-Systeme und müssen sicherstellen, dass ihre Mitarbeiter über ausreichende KI-Kompetenz verfügen, um die Technologie sicher und verantwortungsvoll einzusetzen.
- Kommunen können Anbieter oder Betreiber von KI-Systemen sein. Beide Rollen bringen spezifische Pflichten mit sich, darunter die Erstellung technischer Dokumentationen, Transparenz- und Kennzeichnungspflichten sowie die Haftung für den sicheren Einsatz.
- In Kommunen eingesetzte KI-Systeme müssen nachvollziehbar, sicher und frei von diskriminierenden Verzerrungen sein. Besondere Regelungen gelten für Deepfakes, Emotionserkennung und öffentliche Anwendungen wie Chatbots.
- Nutzer von kommunalen KI-Systemen müssen darüber informiert werden, wenn sie mit einer KI interagieren, und KI-generierte Inhalte müssen klar erkennbar sein. Darüber hinaus sind Maßnahmen zur Verhinderung von Irreführung und Missbrauch erforderlich, insbesondere bei Anwendungen, die direkt mit der Öffentlichkeit interagieren.

b. Datenschutzrechtliche Anforderungen

Wenn beim Einsatz von KI-Systemen personenbezogene Daten verarbeitet werden, müssen Kommunen die datenschutzrechtlichen Vorgaben beachten.

Zusammenfassend gelten dieselben gesetzlichen Anforderungen, die auch für nicht KI-basierte IT-Anwendungen zu erfüllen sind, wenn personenbezogenen Daten verarbeitet werden. So muss die Verarbeitung gemäß Art. 6 DS-GVO rechtmäßig erfolgen. Außerdem wird eine Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) erforderlich, wenn ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht. Die Grundsätze der Datenverarbeitung (Art. 5 DS-GVO), wie Zweckbindung, Datenminimierung und Integrität, sind einzuhalten und es müssen Transparenz- und Informationspflichten (Art. 12-14 DS-GVO) erfüllt werden, um Betroffene über die Datenverarbeitung aufzuklären. Schließlich sind geeignete technisch-organisatorische Maßnahmen (Art. 32 DS-GVO) zu implementieren, um die Sicherheit der Daten zu gewährleisten.

Nachfolgend wird anhand zentraler Vorgaben der DS-GVO geklärt, welche datenschutzrechtlichen Aspekte Kommunen bei KI-Projekten zu beachten haben. Dabei wird kein Anspruch auf

³⁸ KGSt, FAQ AI Act, 2025, S. 15.

Vollständigkeit oder Richtigkeit erhoben. Welche Vorschriften im Einzelfall einschlägig und wie sie anzuwenden sind, hängt von verschiedenen Faktoren wie dem Anwendungsfall und der technischen Implementierung ab. Kommunen sollten daher bei jedem KI-Einsatz frühzeitig ihre Datenschutzbeauftragten einbinden.

Die Verarbeitung personenbezogener Daten muss zunächst auf einer Rechtsgrundlage basieren, wie der Einwilligung der Nutzer (Art. 6 Abs. 1 lit. a DS-GVO) oder der Erfüllung öffentlicher Aufgaben (Art. 6 Abs. 1 lit. e DS-GVO). Vor der Nutzung des Systems ist sicherzustellen, dass die Einwilligung der Nutzer freiwillig, informiert und eindeutig erfolgt. In der Praxis kann das beispielsweise technisch umgesetzt werden, dass eine mit den entsprechenden Informationen versehene Einwilligung erforderlich ist, bevor das KI-System verwendet werden kann. Transparenz spielt eine entscheidende Rolle: Nutzer müssen vorab umfassend über die Datenverarbeitung und ihre Rechte informiert werden, beispielsweise durch eine leicht zugängliche und verständliche Datenschutzerklärung.

Ein zentraler Grundsatz ist die Einhaltung der Datenschutzprinzipien. Dazu gehört die Zweckbindung, wonach Daten nur für die festgelegten und kommunizierten Zwecke verarbeitet werden dürfen. Gleichzeitig ist das Prinzip der Datenminimierung zu beachten, indem nur die Daten erhoben werden, die für den jeweiligen Zweck unbedingt erforderlich sind. Darüber hinaus müssen personenbezogene Daten gelöscht werden, sobald sie für den Zweck nicht mehr benötigt werden oder gesetzliche Aufbewahrungsfristen abgelaufen sind.

Technisch-organisatorische Maßnahmen sind ein weiterer Aspekt, um den Anforderungen an den Datenschutz zu entsprechen. Der Zugang zu den Systemen sollte durch Maßnahmen wie Zwei-Faktor-Authentifizierung und differenzierte Rollen- und Berechtigungskonzepte geschützt werden. Um die Sicherheit personenbezogener Daten weiter zu erhöhen, sollten soweit möglich Pseudonymisierungs- und Anonymisierungstechniken eingesetzt werden. Datenübertragungen zu externen Dienstleistern müssen durch verschlüsselte Verbindungen abgesichert sein, um unbefugten Zugriff zu verhindern.

Die Rechte der betroffenen Personen müssen jederzeit gewährleistet sein. Dazu gehören das Auskunftsrecht, das Recht auf Löschung und das Recht auf Vergessenwerden. KI-Nutzer müssen die Möglichkeit haben, Informationen über die von ihnen gespeicherten Daten anzufordern und deren Löschung zu beantragen, sofern keine gesetzlichen Aufbewahrungsfristen entgegenstehen.

Eine sorgfältige Dokumentation aller datenschutzrelevanten Prozesse und Maßnahmen ist essenziell, um die Nachweisbarkeit gegenüber Aufsichtsbehörden und Nutzern sicherzustellen. Das kann die Dokumentation der Rechtsgrundlagen, der Verarbeitungszwecke sowie der technischen und organisatorischen Maßnahmen umfassen. Ebenso wichtig ist der Abschluss eines Auftragsverarbeitungsvertrags (AVV) mit Dienstleistern, die im Auftrag der Kommune personenbezogene Daten verarbeiten. Dieser Vertrag regelt die Einhaltung der DS-GVO und verpflichtet die Dienstleister zur Umsetzung geeigneter Sicherheitsmaßnahmen. Unterauftragnehmer sollten sorgfältig ausgewählt werden und die marktüblichen Zertifikationen wie ISO 27001 aufweisen. Zudem ist sicherzustellen, dass personenbezogene Daten ausschließlich auf Servern innerhalb der EU verarbeitet werden.

Zusammenfassend ist festzuhalten, dass der Einsatz von KI-Systemen in der kommunalen Verwaltung im Hinblick auf den Datenschutz durch Transparenz, Datensicherheit und die Wahrung der Rechte der Betroffenen geprägt ist.

Um den datenschutzrechtlichen Anforderungen zu entsprechen, können sich Kommunen – unabhängig vom Anwendungsfall – bei der Konzeption von KI-Projekten und bei der Auswahl möglicher Anbieter an den folgenden Punkten orientieren:

- Sie sollten sicherstellen, dass die Ein- und Ausgaben des verwendeten KI-Modells weder für den Anbieter noch für andere Kunden einsehbar sind und nicht zur Verbesserung oder zum Training von KI-Modellen verwendet werden.
- Sie sollten gewährleisten, dass Daten im KI-System ausschließlich im Auftrag und nach den Anweisungen der Kommune verarbeitet werden. Die verwendeten KI-Systeme sollten Eingaben oder generierte Inhalte grundsätzlich nicht dauerhaft speichern oder archivieren. Die Archivierung sollte nur aktiviert werden, soweit dies von der Kommune gewünscht und zur Erfüllung des Anwendungsfalls erforderlich ist. Dabei darf kein Zugriff auf die Daten durch den Anbieter möglich sein.
- Der KI-Dienst sollte vollständig vom Vertragspartner/Anbieter kontrolliert und in einer sicheren, vertrauenswürdigen Umgebung gehostet werden, die den Anforderungen an IT-Sicherheit und Datenschutz entspricht. Das bedeutet beispielsweise, dass mögliche Unterauftragnehmer des Anbieters grundsätzlich keinen Zugriff auf kundenspezifische Daten der Kommune haben dürfen und vertraglich dazu verpflichtet sein müssen, Sicherheitsmaßnahmen einzuhalten – beispielsweise keine Nachrichten zu speichern und Ein- und Ausgaben nicht für Trainingszwecke zu nutzen.
- Kommunen sollten die Möglichkeit haben, Ausnahmen von automatisch aktivierten Überwachungs- oder Prüfmechanismen zu beantragen.

c. Mitbestimmungs- und Mitwirkungsrechte

Bei der Anwendung von KI in der Kommunalverwaltung sind die Mitbestimmungs- und Mitwirkungsrechte der Personalvertretung zu beachten. Sie können beispielsweise die Mitwirkungsrechte bei der Regelung des Verhaltens von Beschäftigten, Einführung grundlegend neuer Arbeitsmethoden oder Maßnahmen zur Hebung der Arbeitsleistung und zur Erleichterung des Arbeitsablaufs betreffen.³⁹ Welche Rechte im Einzelfall zu beachten sind, hängt von verschiedenen Faktoren ab und ist anhand des beabsichtigten Anwendungsfalls oder des Projekts vorab zu prüfen.⁴⁰

Häufig wird eine Kommune feststellen, dass KI nicht nur in einzelnen Projekten eine Rolle spielt, sondern mit der Zeit Einzug in verschiedene IT-Anwendungen und Fachverfahren – ggf. auch kommunale Prozesse und Verwaltungsvorgänge – findet und sich damit zu einer Basistechnologie – vergleichbar mit der schrittweisen Einführung von PC-Arbeitsplätzen und später dem standardmäßigen Internetzugang – entwickelt.

Das bedeutet, dass die Personalvertretung sich nicht nur mit möglichen Auswirkungen auf die Mitarbeiter und ihre Tätigkeit im Einzelfall befassen, sondern im Rahmen ihrer Aufgaben grundlegende Anforderungen und Veränderungen prüfen wird. Im Ergebnis laufen die Abstimmungen zwischen den für KI-Projekte zuständigen Personen und der Personalvertretung oftmals auf den Abschluss einer Dienstvereinbarung hinaus.

³⁹ StMFH Bayern, KI-Leitfaden, 2025, S. 18.

⁴⁰ Ebd.

An dieser Stelle sei angemerkt, dass es bei der Zusammenarbeit mit der Personalvertretung um mehr geht, als die Erfüllung der gesetzlichen Vorgaben. Das Ziel beider Seiten muss darin liegen, den Einsatz von KI zu fördern, gleichzeitig aber disruptive Veränderungen innerhalb der Organisation und Belegschaft zu vermeiden. Beide Seiten müssen gemeinsam den geordneten Übergang in eine durch KI geprägte Arbeitswelt gestalten, in der möglicherweise bestimmte Aufgaben und Tätigkeiten an Bedeutung verlieren oder sich zumindest deutlich verändern.

Für die Nutzung von KI in Kommunen ist festzuhalten:

- KI entwickelt sich zunehmend zu einer Basistechnologie in der Kommunalverwaltung, was eine umfassende Auseinandersetzung mit den Auswirkungen auf Prozesse, Mitarbeiter und Organisation erfordert.
- Bei der Einführung von KI in der Kommunalverwaltung sind die Mitbestimmungs- und Mitwirkungsrechte der Personalvertretung zu beachten. Das kann Regelungen über neue Arbeitsmethoden, Verhaltensregelungen oder Maßnahmen zur Arbeitsoptimierung betreffen.
- Ziel der Zusammenarbeit zwischen Personalvertretung und Verantwortlichen ist es, den KI-Einsatz zu fördern, disruptive Veränderungen zu vermeiden und einen geordneten Übergang in eine KI-geprägte Arbeitswelt zu gestalten.

2. Mögliche Inhalte interner Regelungen

Bislang wurde die Frage beantwortet, welche rechtlichen Vorgaben Kommunen in KI-Projekten zu beachten haben. Offen ist, welche internen Vorgaben Kommunen entwickeln können, um die Nutzung von KI innerhalb ihrer Organisation zu regeln.

Interne Regelungen betreffen im Regelfall Dienstanweisungen oder Dienstvereinbarungen. Sie verfolgen das Ziel, einen für die Beschäftigten verbindlichen Rahmen für die Nutzung von KI-Systemen in einer Kommunalverwaltung zu schaffen.

Allgemein können Kommunen in internen Regelungen verschiedene Aspekte festlegen, um den verantwortungsvollen und sicheren Umgang mit der Technologie zu gewährleisten. Nachfolgend werden beispielhaft mögliche Inhalte beschrieben, die Kommunen in einer Dienstvereinbarung über den Einsatz von KI berücksichtigen können:

1) Grundsätze

Die Kommune kann in einer Dienstvereinbarung zum Einsatz von KI zunächst allgemeine Grundsätze festlegen und damit ihr Verständnis der Technologie und ihrer Zwecke zum Ausdruck bringen.

2) Zweck

Hier kann die Kommune darlegen, was die Ziele der Dienstvereinbarung sind. Beispielsweise kann es um einen sicheren und verantwortungsvollen Umgang mit KI in der Organisation gehen. Ein Ziel kann auch darin liegen, Mitarbeiterinnen und Mitarbeitern Leitlinien für die Nutzung von KI zu bieten.

3) Geltungsbereich

Der Abschnitt beschreibt, für welche Organisationseinheiten, Mitarbeiter und Arbeitsplätze der Kommune die Regelung gilt.

4) *Begriffsbestimmungen*

Die Kommune kann hier relevante Begriffe definieren und dabei Bezug auf die Legaldefinitionen der EU KI-Verordnung nehmen.

5) *Einführung von KI*

Die Kommune kann festlegen, wie die Einführung von KI-Systemen zu erfolgen hat. Sie kann einen Prozess beschreiben oder Einheiten benennen, die zwingend zu beteiligten sind. Die Kommune kann hier außerdem regeln, ob bestimmte KI-Vorhaben (beispielsweise Erprobungen) von der Beteiligungspflicht ausgenommen sind und wie mit nicht freigegebenen KI-Systemen (etwa öffentlich zugänglichen Chatbots) umzugehen ist. Beispielsweise kann verboten werden, dass sich Nutzer mit persönlichen Daten registrieren; stattdessen kann eine Registrierung über bereitgestellte Funktions-Mail-Adressen vorgesehen werden.⁴¹

6) *Verantwortung und Haftung*

Hier kann klargestellt werden, dass die Verantwortung für die korrekte Nutzung von KI-Systemen bei den nutzenden Mitarbeitern liegt. Außerdem kann der erlaubte Nutzungsumfang geregelt werden, beispielsweise, dass die Verwendung von KI ausschließlich auf dienstliche Zwecke und Endgeräte beschränkt ist. Im Hinblick auf die Haftungskonstellation kann die Kommune festschreiben, dass sie keine Haftung für Schäden übernimmt, die durch die Nutzung von KI-Systemen entstehen.

7) *Vertraulichkeit und Datenschutz*

Die Dienstvereinbarung sollte sicherstellen, dass sensible oder vertrauliche Daten nicht in KI-Systeme eingegeben werden dürfen. Je nach technischer Implementierung kann diese Anforderung auf bestimmte KI-Systeme – beispielsweise öffentlich zugängliche – beschränkt werden. Datenschutz und Datensicherheit müssen jedenfalls stets gewährleistet sein. Die Nutzung privater Endgeräte oder Accounts für dienstliche Zwecke kann hier untersagt werden.

8) *Kontrolle und Überprüfung*

Hier kann die Kommune klarstellen, dass die Ausgaben von KI-Systemen vor deren Verwendung in dienstlichen Zusammenhängen stets geprüft werden müssen. Die Regelung muss deutlich machen, dass KI-generierte Inhalte von den Beschäftigten überprüft werden müssen, wobei die Verantwortung für die Richtigkeit und Vollständigkeit der KI-unterstützten Arbeitsergebnisse bei den Nutzern liegt.⁴² Das kann auch den Aspekt der Diskriminierungsfreiheit betreffen.⁴³ Die Regelungen können auch Aussagen über mögliche automatisierte Entscheidungen umfassen, sofern diese in der Kommune Anwendung finden. Um den gesetzlichen Anforderungen zu entsprechen, kann festgelegt werden, dass Inhalte, die mit KI erstellt wurden, entsprechend gekennzeichnet werden müssen, um Transparenz zu gewährleisten.

⁴¹ StMFH Bayern, KI-Leitfaden, 2025, S. 21, 22.

⁴² Gmeinwieser et al. (KGSt/Vitako), Generative KI, 2025, S. 8.

⁴³ Ebd.; StMFH Bayern, KI-Leitfaden, 2025, S. 21, 22.

9) *Qualifizierung*

Die Kommune kann Vorgaben über die KI-Kompetenzen der Mitarbeiter machen. Im Sinne der EU KI-Verordnung kann sie beispielsweise regeln, dass Mitarbeiter, die KI nutzen, über grundlegende Kompetenzen im Umgang mit der Technologie verfügen müssen. Sie kann auch beschreiben, wie ein Nachweis der Kompetenzen erfolgt.

10) *Arbeitsplatzsicherung*

Die Kommune kann regeln, wie mit möglichen Auswirkungen auf die Tätigkeit und das ggf. durch den Einsatz von KI veränderte Aufgabenprofil von Mitarbeitern umgegangen wird. Sie kann festlegen, wo die Verantwortung für die Prüfung von Auswirkungen auf Arbeitsplätze liegt, und welche Einheiten zu beteiligen sind. Die Kommune kann außerdem festlegen, welche Pflichten Mitarbeitern im Hinblick auf Schulungs- und Qualifizierungsangebote zukommen.

11) *Technische Einschränkungen und Support*

Insbesondere mit Bezug zu Pilotprojekten kann die Nutzung von KI technischen Einschränkungen wie Ausfällen oder Fehlfunktionen unterliegen. Es kann geregelt werden, ob, durch wen und in welchem Umfang ein technischer Support für KI-Anwendungen erfolgt.

12) *Weitere Klauseln*

Je nachdem, welche Anwendungsfälle umgesetzt werden, können weitere Regelungen zu erlassen sein. Sie können die Sensibilisierung für mögliche Urheberrechtsverletzungen, Transparenzanforderungen und ethische Aspekte – zum Beispiel mit Blick auf Antidiskriminierung und Gleichstellung – umfassen.⁴⁴ Außerdem können in die Dienstvereinbarung Regelungen über die Gewährleistung von Barrierefreiheit, Informationen über das Inkrafttreten der Vereinbarung und die Rechte der Personalvertretung aufgenommen werden.

3. Zwischenfazit

Festzuhalten ist, dass der rechtliche und organisatorische Rahmen essenziell für einen erfolgreichen und verantwortungsvollen Einsatz von KI-Systemen ist. Die EU KI-Verordnung und das Datenschutzrecht bilden dabei zentrale Grundlagen, die Kommunen sowohl als Anbieter als auch als Betreiber von KI-Systemen beachten müssen. Der risikobasierte Ansatz der Verordnung erfordert eine sorgfältige Bewertung der eingesetzten Systeme, um Transparenz, Sicherheit und Diskriminierungsfreiheit zu gewährleisten.

Darüber hinaus sind interne Regelungen, wie Dienstanweisungen oder Dienstvereinbarungen, ein wichtiges Instrument, um klare Leitlinien für den Umgang mit KI zu schaffen. Sie sollten Aspekte wie Verantwortlichkeiten, Datenschutz, Transparenzpflichten, Schulungen und die Kontrolle von KI-Ausgaben umfassen. Im Rahmen der Einführung und Nutzung von KI-Systemen ist außerdem die Einbindung der Personalvertretung unerlässlich, um Mitbestimmungs- und Mitwirkungsrechte zu wahren und gemeinsam einen geordneten und sozialverträglichen Übergang in eine KI-geprägte Arbeitswelt zu gestalten.

⁴⁴ Gmeinwieser et al. (KGSt/Vitako), Generative KI, 2025, S. 7, 8.

VII. Zusammenfassung

Zu den Einsatzfeldern für KI:

- Kommunen steht schon heute ein breites Spektrum an konkreten KI-Anwendungsfällen zur Verfügung. Sie können KI-gestützte Chatbots einsetzen, um die Kommunikation mit Bürgern zu verbessern, häufig gestellte Fragen zu beantworten und den Zugang zu städtischen Dienstleistungen zu erleichtern.

Zu den Implementierungsoptionen:

- Kommunen sollten mit kleinen, überschaubaren Pilotprojekten beginnen, um erste Erfahrungen mit KI-Technologien zu sammeln und die Akzeptanz zu fördern. Die Wahl der KI-Implementierungsvariante sollte sich an der Größe der Kommune, den verfügbaren personellen und finanziellen Ressourcen, dem IT-Know-how und dem Stand der Digitalisierung orientieren.
- Für die einzelnen Umsetzungsvarianten lässt sich festhalten: Öffentlich zugängliche KI-Systeme bieten niedrige Einstiegshürden, bergen jedoch Risiken bei Datenschutz, Datensicherheit und Anpassbarkeit. Software-Dienste (SaaS) sind flexibel und wartungsarm, können aber langfristig höhere Kosten und Abhängigkeiten verursachen. Cloud-Plattformen ermöglichen Flexibilität und Skalierbarkeit, erfordern jedoch technisches Know-how und eine sorgfältige Vertragsgestaltung.

Zu den Vorgaben der europäischen KI-Verordnung:

- Kommunen müssen KI-Systeme entsprechend ihrer Risikostufe bewerten und die jeweiligen Vorgaben einhalten. Sie tragen die Verantwortung für eingesetzte KI-Systeme und müssen sicherstellen, dass ihre Mitarbeiter über ausreichende KI-Kompetenz verfügen, um die Technologie sicher und verantwortungsvoll einzusetzen.
- Kommunen können Anbieter oder Betreiber von KI-Systemen sein. Beide Rollen bringen spezifische Pflichten mit sich, darunter die Erstellung technischer Dokumentationen, Transparenz- und Kennzeichnungspflichten sowie die Haftung für den sicheren Einsatz.
- Nutzer von kommunalen KI-Systemen müssen darüber informiert werden, wenn sie mit einer KI interagieren, und KI-generierte Inhalte müssen klar erkennbar sein. Darüber hinaus sind Maßnahmen zur Verhinderung von Irreführung und Missbrauch erforderlich, insbesondere bei Ausgaben, die für die Öffentlichkeit bestimmt sind.

Zu den datenschutzrechtlichen Anforderungen:

- Für KI-Anwendungen gelten dieselben gesetzlichen Anforderungen wie für andere IT-Anwendungen, wenn personenbezogene Daten verarbeitet werden. Welche Vorschriften im Einzelfall einschlägig und wie sie anzuwenden sind, hängt von verschiedenen Faktoren wie dem Anwendungsfall und der technischen Implementierung ab.
- Kommunen sollten sicherstellen, dass die Ein- und Ausgaben des verwendeten KI-Modells weder für den Anbieter noch für andere Kunden einsehbar sind und nicht zur Verbesserung oder zum Training von KI-Modellen verwendet werden.

- Sie sollten gewährleisten, dass Daten im KI-System ausschließlich im Auftrag und nach den Anweisungen der Kommune verarbeitet werden. Die verwendeten KI-Systeme sollten Eingaben oder generierte Inhalte grundsätzlich nicht dauerhaft speichern oder archivieren. Der KI-Dienst sollte vollständig vom Vertragspartner/Anbieter kontrolliert und in einer sicheren, vertrauenswürdigen Umgebung gehostet werden, die den Anforderungen an IT-Sicherheit und Datenschutz entspricht.

Zu Mitwirkungs- und Mitbestimmungsrechten der Personalvertretung:

- KI entwickelt sich zunehmend zu einer Basistechnologie in der Kommunalverwaltung, was eine umfassende Auseinandersetzung mit den Auswirkungen auf Prozesse, Mitarbeiter und Organisation erfordert.
- Bei der Einführung von KI in der Kommunalverwaltung sind die Mitbestimmungs- und Mitwirkungsrechte der Personalvertretung zu beachten. Das kann Regelungen über neue Arbeitsmethoden, Verhaltensregelungen oder Maßnahmen zur Arbeitsoptimierung betreffen. Ziel der Zusammenarbeit zwischen Personalvertretung und KI-Verantwortlichen sollte es sein, den KI-Einsatz zu fördern, disruptive Veränderungen zu vermeiden und gemeinsam einen geordneten Übergang in eine KI-geprägte Arbeitswelt zu gestalten.

Zu Anforderungen und Maßnahmen der IT-Sicherheit:

- Für kommunale KI-Projekte können Kommunen die Vorgaben des BSI, insbesondere über den IT-Grundschutz und das Informationssicherheitsmanagementsystem (ISMS), als Grundlage heranziehen. Sie bieten bewährte Methoden und Standards, um die Sicherheit von IT-Systemen – einschließlich KI-Anwendungen – zu gewährleisten.
- Ergänzend hat das BSI Material mit Maßnahmenvorschlägen veröffentlicht, die sich insbesondere auf die sichere Nutzung generativer KI-Modelle konzentrieren. Dazu zählen unter anderem Empfehlungen zur Auswahl geeigneter Modelle, zur Minimierung von Risiken wie Missbrauch oder Manipulation sowie zur Sicherstellung von Transparenz und Erklärbarkeit.
- Der Kriterienkatalog des BSI zum Einsatz generativer KI bietet darüber hinaus eine strukturierte Orientierung für die Integration externer KI-Modelle in kommunale Anwendungen. Er definiert konkrete Maßnahmen für die verschiedenen Projektphasen – von der Planung über die Beschaffung bis hin zur Nutzung und Beendigung.

Zu internen Regelungen für KI:

- Kommunen können interne Vorgaben wie Dienstanweisungen oder Dienstvereinbarungen erlassen, um den Einsatz von KI-Systemen in ihrer Organisation zu regeln. Sie schaffen einen verbindlichen Rahmen für die Beschäftigten und fördern den sicheren, verantwortungsvollen Umgang mit der Technologie.
- Die Regelungen können verschiedene Aspekte abdecken, darunter die Einführung von KI-Systemen, Verantwortlichkeiten und Haftung, Datenschutz und Vertraulichkeit sowie die Kontrolle und Überprüfung von KI-Ergebnissen. Zudem können Vorgaben zur Kennzeichnung von KI-generierten Inhalten, zur Vermeidung von Diskriminierung und zur Sicherstellung der Transparenz gemacht werden.

VIII. Fazit

Kommunen stehen mit der Einführung von KI vor der Chance, ihre Verwaltungsprozesse effizienter zu gestalten, den Bürgerservice zu verbessern und Mitarbeiter durch die Automatisierung von Routineaufgaben zu entlasten. Sie können schon heute in verschiedenen Bereichen auf KI zurückgreifen – etwa durch Chatbots zur Bürgerkommunikation, automatisierte Protokollerstellung, Unterstützung in Antragsprozessen oder die KI-gestützte Dokumentenrecherche. Diese Anwendungen bieten nicht nur Potenziale zur Zeit- und Kostenersparnis, sondern auch zur Verbesserung der Servicequalität und der internen Abläufe.

Für eine erfolgreiche Umsetzung von KI-Projekten ist eine sorgfältige Planung unerlässlich. Kommunen sollten mit Pilotprojekten beginnen, um erste Erfahrungen zu sammeln und die Akzeptanz zu fördern. Die Wahl der technischen Implementierung – sei es durch öffentlich zugängliche KI-Systeme, Software-Dienste oder Cloud-Plattformen – sollte an die individuellen Bedürfnisse, Ressourcen und den Stand der Digitalisierung angepasst werden.

In KI-Projekten müssen Kommunen verschiedene rechtliche Vorgaben wie die EU KI-Verordnung und die Datenschutz-Grundverordnung beachten. Transparenz, Nachvollziehbarkeit und der Schutz personenbezogener Daten sind zentrale Anforderungen, die sie bei der Nutzung von KI-Systemen allgemein berücksichtigen müssen.

Auch die IT-Sicherheit spielt eine entscheidende Rolle. Kommunen können auf bewährte Standards wie den IT-Grundschutz zurückgreifen und ergänzende Maßnahmen ergreifen, um Risiken wie Missbrauch, Manipulation oder fehlerhafte Ergebnisse zu minimieren. Gleichzeitig sollten interne Regelungen geschaffen werden, die den Rahmen für die Nutzung von KI-Systemen verbindlich festlegen.

KI ist eine strategische Basistechnologie für die Modernisierung und Zukunftsfähigkeit der kommunalen Verwaltung. Mit einer durchdachten Strategie, der Einhaltung rechtlicher und technischer Standards sowie der Sensibilisierung und Qualifizierung der Mitarbeiter können Kommunen die Potenziale von KI verantwortungsvoll nutzen und die damit einhergehenden Herausforderungen bewältigen.

Quellen

Alle Links abgerufen am 11.12.2025

Bayerisches Staatsministerium der Finanzen und für Heimat (StMFH Bayern), Einsatz von Künstlicher Intelligenz in der Staatsverwaltung, Leitfaden für Behörden, April 2025, 2. überarbeitete Auflage, abrufbar unter: https://www.stmfh.bayern.de/digitalisierung/ki/KI-Leitfaden_Behoerden_2025.pdf

Bundesamt für Sicherheit in der Informationstechnik (BSI), Generative KI-Modelle: Chancen und Risiken für Industrie und Behörden, 21.01.2025, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Generative_KI-Modelle.html

Ebd., ISMS.1 Sicherheitsmanagement, Edition 2023, 01.02.2023, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium Einzel PDFs 2023/01 ISMS Sicherheitsmanagement/ISMS_1 Sicherheitsmanagement Edition 2023.html

Ebd., Kriterienkatalog zum Einsatz generativer KI in der Bundesverwaltung, Version 1, 06.06.2025, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Kriterienkatalog_KI-Modelle_Bundesverwaltung.pdf?__blob=publicationFile&v=3

Ebd., Lerneinheit 5.2: Schichtenmodell, abrufbar unter: <https://www.bsi.bund.de/dok/10990558>

Gmeinwieser, J./Baltissen, A./Krellmann, A./Hörmeyer, M./Hoppmann, L./Giebel, K./Hedde, P./Hensel, L., (VITAKO Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e.V./ Kommunale Gemeinschaftsstelle für Verwaltungsmanagement (KGSt)/ Prosoz Herthen GmbH), Generative KI in Kommunalverwaltungen, Guideline und praktische Anwendungsfälle für Large Language Modelle, September 2025, abrufbar unter: <https://www.kgst.de/generative-ki-in-kommunalverwaltungen>

Hassan, H./Aue, A./Chen, C./Chowdhary, V./Clark, J./Federmann, C./Huang, X./Junczys-Dowmunt, M./Lewis, W./Li, M./Liu, S./Liu, T.-Y./Luo, R./Menezes, A./Qin, T./Seide, F./Tan, X./Tian, F./Wu, L./Wu, S./Xia, Y./Zhang, D./Zhang, Z./Zhou, M., Achieving Human Parity on Automatic Chinese to English News Translation, revised Jun. 2018, abrufbar unter: <https://arxiv.org/abs/1803.05567>

He, K./Zhang, X./Ren, S./Sun, J., Delving Deep into Rectifiers: Surpassing Human-Level Performance on ImageNet Classification, 2015 IEEE International Conference on Computer Vision, DOI: 10.1109/ICCV.2015.123

Hu, X./Yin, X./Lin, K./Wang, L./Zhang, L./Gao, J./Liu, Z., VIVO: Visual Vocabulary Pre-Training for Novel Object Captioning, revised Mar. 2021, abrufbar unter: <https://arxiv.org/abs/2009.13682>

Josipovic, N., Beispiele für den Einsatz von großen Sprachmodellen (LLM) in der Landes- und Kommunalverwaltung, Arbeitspapier vom 30.10.2025, abrufbar unter: <https://neven-josipovic.de/index.php/publikationen>

Ebd., KI-basierte Auswertung kommunaler Daten mit dem GPT Data Analyzer, Arbeitspapier vom 12.10.2023, abrufbar unter: <https://nevenjosipovic.de/index.php/publikationen>

Kommunalen Gemeinschaftsstelle für Verwaltungsmanagement (KGSt), FAQ EU AI Act, Publikation Nr. 11/2025, abrufbar unter: https://www.kgst.de/dokumentdetails?path=/documents/20181/13218725/P-11-2025_FAQ-EU-AI-Act.pdf/93857b46-56aa-aa06-c192-eabb01a6e937?t=1761746445400

Marr, B., ChatGPT: What Are Hallucinations And Why Are They A Problem For AI Systems, Online-Beitrag vom 22.03.2023, abrufbar unter: <https://bernardmarr.com/chatgpt-what-are-hallucinations-and-why-are-they-a-problem-for-ai-systems/>

McKinsey (GenAI 2024), Mit Mut und Augenmaß, bitte! Wie GenAI die Arbeit der öffentlichen Verwaltung unterstützen und den Fachkräftemangel abfedern kann, Juli 2024, abrufbar unter: https://www.mckinsey.com/de/~/_/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2024/2024-07-15%20genai%20and%20talent%20in%20public%20sector/mckinseymit%20mut%20und%20augen-mass%20bitte.pdf

Microsoft, Schatten-KI macht Deutschland verwundbar: Microsoft-Studie zeigt Schutzlücke in Behörden, Online-Beitrag vom 11.11.2025, abrufbar unter: <https://news.microsoft.com/source/emea/2025/11/schatten-ki-macht-deutschland-verwundbar-microsoft-studie-zeigt-schutzluecke-in-behoerden/?lang=de>

Ebd., Shared responsibility in the cloud, Online-Beitrag vom 03.12.2025, abrufbar unter: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

SAP, Was ist Machine Learning?, abrufbar unter: <https://www.sap.com/germany/products/artificial-intelligence/what-is-machine-learning.html>

TÜV Rheinland, Klassifikation von KI: Die vier Risikostufen des EU AI Act, Online-Beitrag vom 18.02.2025, abrufbar unter: <https://consulting.tuv.com/aktuelles/ki-im-fokus/klassifikation-von-ki-die-vier-risikostufen-des-eu-ai-act>

Xiong, W./Droppo, J./Huang, X./Seide, F./Seltzer, M./Stolcke, A./Yu, D./Zweig, G., Achieving Human Parity in Conversational Speech Recognition, MSR-TR-2016-71, revised Feb. 2017, abrufbar unter: <https://arxiv.org/abs/1610.05256>

Anhang: Auszug aus dem BSI-Kriterienkatalog

| MUSS-Maßnahmen | SOLL-Maßnahmen |
|--|---|
| Globale KI-Governance | |
| Einen KI-Zuständigen benennen. | Übersicht sollte interne Anpassungen und Zugriffsrechte des KI-Modells dokumentieren. |
| Übersicht aller KI-Anwendungen erstellen. | Übersicht sollte zur Information der internen Endnutzenden über KI-Anwendungen genutzt werden. |
| Neu eingeführte Anwendungen in die Übersicht aufnehmen. | Einen Prozess zum Schwachstellenmanagement definieren. |
| Verantwortliche für jede Anwendung in der Übersicht angeben. | Anwendungen regelmäßig und anlassbezogen auf Schwachstellen prüfen. |
| Verwendete KI-Modelle und erlaubte Anwendungsfälle in der Übersicht dokumentieren. | Neuartige Bedrohungen und Änderungen bei existierenden Bedrohungen berücksichtigen. |
| Übersicht zur schnellen Feststellung von Schwachstellen nutzen. | Endnutzende sollten sich mit den Funktionalitäten der Anwendung vertraut machen. |
| Nutzungsbedingungen für Anwendungen erstellen und bereitstellen. | Eingaben der Endnutzenden sollten präzise und sprachlich korrekt formuliert werden. |
| Anwendungsfälle und Nutzungsbedingungen regelmäßig (mind. jährlich) überprüfen. | Ausgaben oder daraus gewonnene Informationen sollten als KI-generiert gekennzeichnet werden (falls erforderlich). |
| Schulung/Sensibilisierung der Endnutzenden sicherstellen. | Regelungen der Nutzungsbedingungen sollten in Schulungen oder Dokumenten vermittelt werden. |
| Sensible Daten nur bei Notwendigkeit und Erlaubnis verarbeiten. | |
| Eingaben der Endnutzenden müssen den erlaubten Zwecken dienen. | |
| Risikobewusster Umgang mit Ausgaben sicherstellen. | |
| Kontaktmöglichkeit für Endnutzende bereitstellen. | |
| Datenschutzbeauftragte bei Datenschutzentscheidungen einbeziehen. | |
| Geheimhaltungsbeauftragte bei Geheimhaltungsentscheidungen einbeziehen. | |
| Mindeststandard Cloud-Nutzung bei Cloud-basierten Modellen beachten. | |
| Anwendungsfallbezogene Planungsphase | |
| Anwendungsfall klar definieren. | Aus jedem relevanten KI-Risiko sollte mindestens ein Auswahlkriterium für das KI-Modell abgeleitet werden. |
| Auswahlkriterien für die Modellauswahl festlegen. | |
| Relevante KI-Risiken identifizieren. | |
| Keine relevanten KI-Risiken? Begründung dokumentieren. | |
| Kriterien zur Bewertung der Vertrauenswürdigkeit von Anbietern definieren. | |
| Obligatorische und optionale Kriterien festlegen. | |

| Beschaffungsphase | |
|--|--|
| KI-Modell anhand der Planungsphase-Kriterien beurteilen. | Informationen des Anbieters (z. B. Nutzungsbedingungen, Model-Cards, Benchmark-Tests) sollten gesichtet werden. |
| AIC4-/AICM-Testat auswerten und beurteilen. | Informationen Dritter zur Beurteilung des KI-Modells sollten genutzt werden. |
| Auswahl des KI-Modells begründen. | Eigene Tests (z. B. Benchmarks, Red Teaming) sollten durchgeführt werden. |
| Modell aus vertrauenswürdigen Quellen beziehen. | Anbieter sollte zusichern, dass bereitgestellte Informationen nicht für andere Zwecke (z. B. Training) verwendet werden. |
| Mindeststandard Cloud-Nutzung bei Cloud-basierten Modellen beachten. | Signaturen sollten geprüft und sichere Formate genutzt werden. |
| IT-Sicherheitsmaßnahmen bei lokalem Betrieb umsetzen. | AIC4-/AICM-Testat sollte als Nachweis der Vertrauenswürdigkeit der Quelle genutzt werden (falls vorhanden). |
| Anpassungsphase | |
| IT-Sicherheitsmaßnahmen beim Bezug weiterer Komponenten umsetzen. | System-Prompts sollten zentral verwaltet und Änderungen nachverfolgbar sein. |
| Keine sensiblen Daten in System-Prompts integrieren. | System-Prompts sollten nicht zur Umsetzung eines Rechte-/Rollensystems genutzt werden. |
| Bewusstsein für Umgehung von System-Prompts (Prompt Injections) sicherstellen. | |
| Integrationsphase | |
| Anwendung ins ISMS integrieren. | Threat Modelling sollte durchgeführt werden, um Integrationsrisiken zu identifizieren. |
| Tests zur Überprüfung der identifizierten Risiken durchführen. | Maßnahmen zur Absicherung der Integration sollten ergriffen werden, z. B. Umsetzung eines Rechte- und Rollenkonzepts. |
| Testergebnisse dokumentieren. | |
| Dokumentation muss zeigen, ob bei neuen Bedrohungen erneut getestet werden muss. | |
| Bei schlechten Testergebnissen vorherige Phasen wiederholen. | |
| Einsatzphase | |
| Mindeststandard Cloud-Nutzung bei Cloud-basierten Modellen beachten. | Zugriff auf die Anwendung sollte auf das notwendige Minimum beschränkt werden (insbesondere bei externer Nutzung). |
| Endnutzenden ersichtlich machen, dass KI-Komponenten verwendet werden. | Wichtige Regelungen der Nutzungsbedingungen sollten an auffälliger Position in der Anwendung dargestellt werden. |
| Maßnahmen gegen missbräuchliche Nutzung der Anwendung umsetzen. | Anwendungsspezifische Schulungen sollten angeboten werden. |
| Beendigungsphase | |
| Mindeststandard Cloud-Nutzung bei Cloud-basierten Modellen beachten. | |
| Sensible Daten vor Weiterverwendung der Anwendung entfernen. | |