

CSBW

CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

Künstliche Intelligenz (KI) in der kommunalen Verwaltung

Die Integration von künstlicher Intelligenz (KI) in den Arbeitsalltag der kommunalen Verwaltung bietet vielfältige Möglichkeiten zur Prozessoptimierung und Effizienzsteigerung. Dieses Factsheet beleuchtet sowohl die Potenziale als auch die Herausforderungen beim Einsatz von KI-Technologien in der öffentlichen Verwaltung.

Was sollte eine Kommune vor dem Einsatz von KI beachten?



Anwendungsbereiche von KI

Die Anwendungsbereiche von KI innerhalb der kommunalen Verwaltung sind breit gefächert.

Der Einsatz von KI ist unter anderem in folgenden Bereichen möglich:

- ▶ Automatische Rechtschreibkorrektur
- ▶ Erstellung von Übersetzungen
- ▶ Intelligente E-Mail-Verteilung
- ▶ KI-gestützte Bildgenerierung für Marketingzwecke
- ▶ Chatbots und persönliche Sprachassistenten
- ▶ Service-Roboter als digitale Assistenten
- ▶ Förderung der digitalen Barrierefreiheit
- ▶ Wissensmanagement
- ▶ Abwehr von Cyberangriffen

KI in der öffentlichen Verwaltung¹

Der Einsatz von KI in der öffentlichen Verwaltung verspricht mehrere Vorteile:

- ▶ Effizienzsteigerung bei Verwaltungsabläufen
- ▶ Verbesserte Kommunikation mit Bürgerinnen und Bürgern
- ▶ Reduzierung der Arbeitsbelastung für Verwaltungsmitarbeitende
- ▶ Beschleunigung von Verwaltungsdienstleistungen
- ▶ Ressourcenschonung durch Automatisierung

Aufgrund der Sensibilität und des hohen Schutzbearbedarfs der in der Verwaltung verarbeiteten personenbezogenen Daten ist jedoch eine sorgfältige rechtliche und technische Absicherung beim Einsatz von KI unerlässlich.

Überlegungen vor dem Einsatz von KI²

Die folgenden Schlüsselfragen sollen als Denkanstöße vor dem Einsatz von KI-Systemen dienen:

1. **Realistische Erwartungen:** Vor der Implementierung sollte sorgfältig geprüft werden, ob das gewählte KI-Modell für die angestrebte Aufgabe geeignet ist und auf Basis welcher Daten das Modell trainiert wurde.
2. **Offene Kommunikation:** Bürgerinnen und Bürger sollten darüber informiert werden, in welchen Bereichen und bei welchen Dienstleistungen KI zum Einsatz kommt.
3. **Transparenz der Fehleranfälligkeit:** Es ist wichtig, klar zu kommunizieren, dass KI-Systeme Fehler ausgeben können. Falls die Eingaben der Nutzer zum Training und Verbesserung des KI-Systems verwendet werden, müssen diese ebenfalls darauf hingewiesen werden.
4. **Umgang mit KI-Halluzinationen:** Strategien zur Erkennung und Handhabung von KI-generierten Fehlinformationen sind zu entwickeln. So sollte beispielsweise bei kritischen Prozessen eine manuelle Endkontrolle stattfinden.
5. **Akzeptanzförderung:** Maßnahmen zur Steigerung der Akzeptanz von KI-gestützten Dienstleistungen bei Bürgerinnen und Bürgern sollten ergriffen werden.
6. **IT-Sicherheit:** Schutzmaßnahmen gegen Angriffe wie Prompt-Hijacking sind zu implementieren. Zusätzlich kann eine durchdachte Architektur Angriffe oder Informationsabfluss verhindern, beispielsweise indem getrennte Modelle für interne und externe Aufgaben verwendet werden.
7. **Missbrauchsprävention:** Vorkehrungen gegen den Einsatz von KI für Desinformation, Social Engineering oder die Optimierung von Cyberangriffen sind zu treffen.
8. **Rechtliche Aspekte:** Die Haftungsfrage im Schadensfall muss geklärt sein.
9. **Datenschutz und -sicherheit:** Die Herkunft der Trainingsdaten sowie die Verarbeitung und potenzielle Weiterverwendung von Nutzerdaten müssen transparent gemacht werden.
10. **Regulatorische Compliance:** Die Einhaltung der KI-Verordnung und anderer relevanter Gesetze muss sichergestellt sein.
11. **Ethische Überlegungen:** Die Auswirkungen des KI-Einsatzes auf Fairness, Gleichberechtigung und soziale Gerechtigkeit müssen berücksichtigt werden.
12. **Schulung und Weiterbildung:** Mitarbeiter der Verwaltung sollten im Umgang mit KI-Systemen geschult werden, um deren Potenzial optimal zu nutzen und mögliche Risiken zu minimieren.
13. **Prüfung des Einsatzzwecks:** Vorüberlegungen treffen, ob für den geplanten Einsatzzweck ein eigenes Modell trainiert wird (BYO-LLM) oder ein bereits bestehendes genutzt werden kann.
14. **Grenzen vollautomatischer Entscheidungen beachten:** Den gesetzlichen Rahmen einhalten gem. § 35 VwVfG, Art. 22 DSGVO.

Quellen:

¹ <https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/datenpolitik/daten-und-ki/daten-und-ki-node.html>

² <https://www.europarl.europa.eu/topics/de/article/20200918STO87404/kunstliche-intelligenz-chancen-und-risiken>

