



Stand 30. August 2023

## 1. Zweck und Gegenstand dieses Merkblatts

Die hohe Dynamik von Online-KI-Generatoren und ihre potenziellen Chancen und Risiken führen zu verschiedenen rechtlichen Fragen. Ihre Beantwortung kann im Anwendungsfall anspruchsvoll sein. Dieses Merkblatt soll eine erste Orientierung ermöglichen, was Mitarbeitende der kantonalen Verwaltung bei der Nutzung von Online-KI-Generatoren in rechtlicher Hinsicht zu beachten haben. Es richtet sich an alle Mitarbeitenden der Direktionen und der Staatskanzlei, die Online-KI-Generatoren im Rahmen ihrer Erfüllung von Verwaltungsaufgaben für den Kanton Zürich nutzen möchten.

Dieses Merkblatt ist auf die Nutzung von Textgeneratoren ausgerichtet. Die hier dargelegten Grundsätze gelten sinngemäss aber auch im Zusammenhang mit der Generierung von Bildern, Programmcode usw. Das Merkblatt ist eine Hilfestellung; ausschlaggebend ist das geltende Recht.

Nicht Gegenstand des vorliegenden Merkblatts ist der Einsatz eigener, durch die Verwaltung entwickelter bzw. kontrollierter KI-basierter Anwendungen (z.B. [Chatbot Lohnabrechnung](#); [Innovation Sandbox](#)) sowie die Nutzung von Online-KI-Generatoren zu Bildungszwecken an Schulen und Universitäten und deren Einsatz in der Forschung.

## 2. Was sind Online-KI-Generatoren?

Die Leistungsfähigkeit KI-basierter Anwendungen schreitet schnell voran. Derzeit im Fokus stehen online öffentlich zugängliche generative KI-Anwendungen in der Form von Textgeneratoren wie z.B. ChatGPT oder Google Bard. Dabei handelt es sich um im Internet (frei oder nach Registrierung) zugängliche Anwendungen, welche den Text einer Eingabe analysieren und darauf basierend automatisch einen Text als Ausgabe generieren (vergleichbare Anwendungen gibt es auch für die Generierung von Grafiken, Bildern, Musik usw.). Im Folgenden werden diese Anwendungen, die derzeit von verschiedenen Anbietern online zugänglich gemacht werden, als Online-KI-Generatoren bezeichnet.

## 3. Welche rechtlichen Vorgaben sind zu beachten?

Wie bei der Nutzung von jedem Informatikmittel sind auch für Online-KI-Generatoren die allgemeinen rechtlichen Vorgaben bezüglich Vertraulichkeit, Informationssicherheit und Datenschutz zu beachten. Diese Vorgaben gelten unverändert auch bei der Nutzung von Online-KI-Generatoren.

Zu berücksichtigen sind insbesondere:

- der Schutz von Personendaten (siehe Gesetz über die Information und den Datenschutz [IDG, LS 170.4] und Art. 13 Bundesverfassung [SR 101]);
- die Sicherheit von Daten (siehe IDG, Verordnung über die Informationsverwaltung und -sicherheit [LS 170.8] u.a.);
- die Wahrung des Amtsgeheimnisses (siehe Schweizerisches Strafgesetzbuch [SR 311.0] u.a.);
- personalrechtliche Pflichten (siehe Personalgesetz [LS 177.10]) sowie
- spezifische Vorgaben über die Nutzung von Informatikmitteln.

Je nach Anwendungsfall können weitere Vorgaben, etwa zu Urheberrechten, beachtlich sein.



#### **4. Wofür eignen sich Online-KI-Generatoren?**

Aufgrund der Funktionsweise von Online-KI-Generatoren, der Nutzungsbedingungen der Anbieter und der rechtlichen Vorgaben des Kantons eignen sich Online-KI-Generatoren in der Regel vorwiegend als Arbeitshilfe zum persönlichen Gebrauch. Gewisse Risiken lassen sich reduzieren, sofern bei der Nutzung von Online-KI-Generatoren nur auf öffentlich zugängliche Informationen zurückgegriffen wird.

Unproblematische Nutzungsmöglichkeiten umfassen z.B. (unter Beachtung der oben genannten Vorgaben)

- das Erstellen einer Zusammenfassung von öffentlich zugänglichen Informationen,
- die Nutzung für ein Brainstorming zu allgemeinen Themen,
- die Nutzung als Formulierungshilfe für allgemeine eigene Texte, für E-Mails ohne Personendaten oder vertraulichen Inhalt usw.

Hingegen ist die Nutzung von Online-KI-Generatoren für viele Verwaltungsaufgaben nicht geeignet. Von der Nutzung von Online-KI-Generatoren sollte grundsätzlich abgesehen werden

- im Austausch mit der Bevölkerung (z.B. bei der Beantwortung von Anfragen),
- zum Vorbereiten von rechtsverbindlichen Entscheiden (z.B. Erlass einer Verfügung) oder
- zum Erarbeiten von Arbeitsdokumenten basierend auf verwaltungsinternen Informationen.

Vor einem spezifischen Einsatz von KI-basierten Hilfsmitteln für die Bearbeitung von Verwaltungsaufgaben sollte anhand des konkreten Anwendungsfalles eine Rechtsgrundlagenanalyse vorgenommen und gegebenenfalls das Verfahren gemäss IDG (wie Datenschutz-Folgenabschätzung, ISDS und Vorabkontrolle) eingehalten werden.

#### **5. Was ist bei der Nutzung von Online-KI-Generatoren generell zu beachten?**

Interne, vertrauliche und geheime Informationen der Verwaltung sowie Personendaten generell dürfen nicht in Online-KI-Generatoren eingegeben werden. Beachten Sie, dass selbst anonymisierte Informationen Rückschlüsse auf Personen sowie auf nicht öffentliche Informationen der Verwaltung ermöglichen können. Solche Informationen dürfen nicht ohne Weiteres an Dritte (d.h. an die Anbieter) bekannt gegeben werden.

Prüfen Sie in jedem Einzelfall, ob Sie berechtigt sind, die von Ihnen verwendeten Daten der Verwaltung an den Anbieter zu übermitteln.

Bedenken Sie bei der Nutzung von Online-KI-Generatoren zudem, dass

- die Nutzungsbedingungen weitreichende Pflichten und Einschränkungen vorsehen können (z.B. bezüglich der Verwendung der Ergebnisse),
- Sie durch Ihre Eingaben dem Anbieter verschiedenste Daten mitteilen, die damit den Kontrollbereich der Verwaltung verlassen,
- Die von Ihnen eingegebenen Informationen vom Anbieter u.U. für dessen eigene Zwecke (z.B. zur Produktentwicklung) ausgewertet oder anderweitig kommerzialisiert werden können.



## **6. Was ist bei der Eröffnung des Nutzungskontos zu beachten?**

Für die Nutzung von Online-KI-Generatoren (wie z.B. ChatGPT oder Google Bard) muss beim entsprechenden Anbieter zumeist eine Registrierung erfolgen bzw. ein Nutzungskonto eröffnet werden. Damit kann die Zustimmung zu den Nutzungsbedingungen des Anbieters verbunden sein. Dadurch gehen die Nutzenden einen Vertrag mit dem Anbieter ein, in welchem sie dem Anbieter unter Umständen weitgehende Rechte (z.B. an den übermittelten Informationen) einräumen und ihnen der Anbieter gewisse Nutzungsvorgaben und Einschränkungen auferlegt. Die Vorgaben solcher Nutzungsbedingungen können insbesondere den informations- und datenschutzrechtlichen Vorgaben widersprechen, die bei der Erfüllung von Verwaltungsaufgaben zu beachten sind.

Bei der Registrierung ist insbesondere zu beachten:

- Verwenden Sie für die Registrierung *nicht* Ihre geschäftlichen Angaben (wie E-Mail-Adresse, Telefonnummer usw.).
- Beachten Sie, dass die bei der Registrierung eingegebenen Personendaten den Datenschutzbestimmungen am Sitz des jeweiligen Anbieters unterstehen (die unter Umständen weniger Schutz bieten als das Schweizer Datenschutzrecht).
- Schränken Sie die Verwendung der eingegebenen Daten durch den Anbieter in den Einstellungen Ihres Nutzungskontos so weit wie möglich ein.

## **7. Was ist bei der Eingabe von Informationen zu beachten?**

Bei der Eingabe von Informationen im Eingabefeld (Prompt) eines Online-KI-Generators ist insbesondere Folgendes zu beachten:

- Die Eingabe darf keine Personendaten enthalten (d.h. Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen); beachten Sie dabei, dass selbst anonymisierte Informationen unter Umständen Rückschlüsse auf Personen ermöglichen können.
- Die Eingabe darf keine Informationen enthalten, welche der Organisationseinheit zugeordnet werden können (wie z.B. Abteilungsbezeichnungen, interne Kennungen, Aktenzeichen usw.).
- Die Eingabe darf keine als intern, vertraulich oder geheim klassifizierten Informationen enthalten. Gehen Sie bei Unsicherheiten über die Zuordnung immer von der höheren anwendbaren Schutzklasse aus.
- Generell darf die Eingabe keine Informationen enthalten, welche die Organisationseinheit nicht verlassen dürfen (wie etwa nicht öffentliche Anfragen aus der Bevölkerung oder Ausschnitte davon).

## **8. Was ist bei der Verwendung der Ergebnisse zu beachten?**

Die Ausgabe eines Online-KI-Generators basiert auf Wahrscheinlichkeitsberechnungen, d.h. die Ausgabe ist nur (rechnerisch) «wahrscheinlich» und nicht notwendigerweise auch (inhaltlich) korrekt. Identische Eingaben können zudem zu unterschiedlichen Ausgaben führen: Auch wenn mehrmals dieselbe Frage eingegeben wird, werden allenfalls jedes Mal andere Ergebnisse generiert (sogenannte fehlende Reproduzierbarkeit).



Bedenken Sie bei der Nutzung von Online-KI-Generatoren deshalb, dass

- die angezeigten Ergebnisse gerade bei komplexeren Inhalten vielfach nicht korrekt oder unvollständig sind,
- eine Überprüfung entsprechende Fachkenntnisse voraussetzt und
- die angezeigten Ergebnisse dennoch überzeugend klingen und sich teilweise kaum von solchen unterscheiden lassen, die selbstständig von Menschen erarbeitet wurden.

Die mit Online-KI-Generatoren erzeugten Ergebnisse sollten lediglich zur Unterstützung und nicht als Ersatz für die eigene Arbeitsleistung verwendet werden:

- Hinterfragen und verifizieren Sie sämtliche Ergebnisse. Betrachten Sie diese als erste Anregung und Einstiegspunkt für die weitere eigene Bearbeitung.
- Verwenden Sie nur solche Ergebnisse, deren Korrektheit und Angemessenheit Sie aufgrund Ihrer eigenen Fachkenntnisse beurteilen können.
- Diskutieren Sie die Ergebnisse und die dabei gewonnenen Erkenntnisse mit Ihren Fachkolleginnen und Fachkollegen.

## **9. Wann und wie sind die verwendeten Ergebnisse zu kennzeichnen?**

Die Nutzung von Online-KI-Generatoren muss transparent erfolgen. Ergebnisse, die mit Hilfe von Online-KI-Generatoren erstellt wurden und ohne substantielle Überarbeitung übernommen werden, sind entsprechend zu kennzeichnen. Diese Kennzeichnung soll den Empfängerkreis (z.B. eines Dokuments) informieren, dass ein Online-KI-Generator und somit eine relativ neue Arbeitshilfe genutzt wurde.

Falls Sie Ergebnisse von Online-KI-Generatoren (nach erfolgter Verifikation, siehe oben) ohne substantielle Anpassungen verwenden:

- Kennzeichnen Sie diese klar und unmissverständlich als unter Mithilfe von KI-Hilfsmitteln erstellt. Beachten Sie dabei allfällige Vorgaben aus den Nutzungsbedingungen des Anbieters.
- Ein solcher Hinweis sollte nach eigener Einschätzung an einer passenden Stelle im Dokument angebracht werden, wie etwa in Form einer Quellenangabe, einer Fuss- oder Endnote oder eines pauschalen Hinweises zu Beginn des Dokuments.
- Der Hinweis sollte den Umfang und die Art und Weise der Verwendung von Online-KI-Generatoren transparent darlegen (Beispiel: «Der Text in Abschnitt [betroffene Textstelle] wurde mit Hilfe von [verwendeter Online-KI-Generator] in der Version [verwendete Version des Online-KI-Generators] erstellt und von der Autorin / vom Autor nach inhaltlicher Prüfung [mit gewissen Anpassungen] übernommen»).

## **10. Kontakt für Fragen und weitere Informationen**

Bei weiteren Fragen oder Unklarheiten wenden Sie sich bitte an:  
Staatskanzlei, Digitale Verwaltung (DVE), Abteilung Recht

Beachten Sie für weitere Anpassungen und Informationen zur Nutzung von Online-KI-Generatoren die üblichen Kommunikationskanäle des Kantons und der Direktionen.