KI-TRANSPARENZBERICHT NEOS LINZ

Berichtszeitraum: 01.01.2025 – 02.06.2025
Veröffentlichungsdatum: 02.06.2025

1. Einleitung

Im Sinne unserer ethischen Standards und unseres Versprechens an die Bürger:innen von Linz legen wir mit diesem Bericht offen, wie NEOS Linz Künstliche Intelligenz in der politischen Arbeit einsetzt. Ziel ist es, Transparenz zu schaffen, Vertrauen zu stärken und kontinuierliche Verbesserung zu ermöglichen.

2. Unsere Grundsätze

Wir setzen KI ausschließlich nach den folgenden Grundsätzen ein:

- Verantwortung bleibt immer beim Menschen.
- Transparenz und Kennzeichnung von KI-Inhalten bei audiovisuellen Medien.
- Einhaltung des EU AI Act und der DSGVO.
- Verzicht auf manipulative Praktiken.

3. Verwendete KI-Werkzeuge im Berichtszeitraum

Berichtszeitraum: 01-06 2025			
Tool / Anbieter	**Zweck / Einsatzgebiet**	**Risiko-Klassifizierung (EU AI Act)**	**Kennzeichnung**
ChatGPT / OpenAI]	Vorschlag für Texte Umsetzung individuell	Minimales Risiko	nicht erforderlich
	Audio | Video	Geringes Risiko	JA
	Interne Analysen	Geringes Risiko	JA (intern)
	SoMe Posting Unterstützung bei CAPTIONS (Vorschlag) Umsetzung individuell	Minimales Risiko	nicht erforderlich
Canva Magic Write	Postings	Minimales Risiko	nicht erforderlich
Perplexity	Recherche	Minimales Risiko	nicht erforderlich
Livansa	Audio | Video	Geringes Risiko	JA
Grok	Unterstützung Textgenerierung	Minimales Risiko	nicht erforderlich
AISong	Audiogenerierung	Geringes Risiko	JA
Parrot	Audio | Video	Geringes Risiko	JA
Dreamina	Audio | Video	Geringes Risiko	JA

4. Konkrete Anwendungsfälle

4.1 Beschreibung der Einsätze

- Unterstützung bei der Formulierung von Texten, Social Media Beiträgen (Vorschlag Hashtags, Captions)
- Texterstellung, Zusammenfassungen, Analysen
- Unterstützung bei der Erstellung von Texten in einfacher Sprache
- Korrekturlesen

4.2 Kennzeichnung

- Alle durch KI unterstützten audiovisuellen Inhalte wurden mit Hinweisen wie „Erstellt mit Unterstützung von KI“ oder „AI generated“ gekennzeichnet.

5. Evaluierung der KI-Einsätze

5.1 Erkenntnisse

- Der Einsatz von KI hat die Qualität der verwendeten Schriftsätze und Posting erheblich verbessert.
- Die Analyse der politischen Arbeit von öffentlich verfügbaren Dokumenten macht die Arbeit sehr effizient und gibt uns Freiraum zur Bewertung und kreativen Umsetzungen.

5.2 Positivbeispiele

- Social Media Postings
- Redigieren von Texten
- Analyse öffentlich zugänglicher Dokumente

5.3 Verbesserungspotenziale

- Antworten der KI-Tools sollten auf Plausibilität überprüft werden. Immer nach Quellenangaben fragen.
- Sensibilisierung des Teams für die Prüfung von Inhalten.
- Werden Texte 1:1 übernommen, müssen sie gekennzeichnet werden. Vorschläge: „#AIgenerated“ oder „Unterstützt von KI“.

6. Feedback und Beschwerden

6.1 Rückmeldungen

- Qualität der Captions wurde als fehlerlos bewertet.
- EU AI Act Regularien sind nicht immer klar
- Anwendung der KI-Tools ist nicht durchgehend transparent

6.2 Reaktionen und Maßnahmen

- Ausweitung KI-Kompetenz im Team durch gezielte Schulungen

7. Fortbildungen und Sensibilisierungen

Geplant: KI-Workshop (Einführung KI, Zertifikat EU AI Act) – Juli/August 2025

8. Ausblick

Das Thema KI wird weiterhin Bestandteil regelmäßiger Teammeetings und Fortbildungen sein.

9. Impressum / Kontakt

Herausgeber: NEOS Linz
Verantwortlich: Mag. Georg Redlhammer, Fraktionsvorsitz
Kontakt: georg.redlhammer@neos.eu
Webseite: https://oberoesterreich.neos.eu/gemeinden/linz

Erstellt im Einklang mit den "Ethischen Standards für den Einsatz von KI bei NEOS Linz" und den "Nutzungsrichtlinien für KI-Werkzeuge bei NEOS Linz" (Stand Juni 2025).

Georg Redlhammer
Gemeinderat/ Fraktionsvorsitz

Stefan Burgstaller
Gemeinderat

ANHANG

Risiko-Klassifizierung gemäß EU AI Act zusammengefasst:

✅ 1. Minimales Risiko (Erlaubt ohne Auflagen)

- Beispiele:
  - Rechtschreibprüfung
  - Spam-Filter
  - Empfehlungssysteme für Filme, Musik
- Kein spezielles Risiko für Grundrechte, Gesundheit oder Sicherheit.

⚠️ 2. Geringes Risiko (Informationspflicht)

- Beispiele:
  - Chatbots, die keine reale Person sind (müssen als KI erkennbar sein)
  - KI-generierte Bilder/Videos, die nicht täuschen dürfen
- Kennzeichnungspflicht für Nutzer:innen erforderlich.

⚠️ 3. Hohes Risiko (strenge Auflagen)

- Beispiele:
  - KI in kritischer Infrastruktur (z.B. Wasser, Energieversorgung)
  - KI in Personalrekrutierung (Bewerbungsscreening)
  - KI in Bildung (Bewertung von Prüfungen)
  - KI in der öffentlichen Verwaltung (z.B. Sozialleistungen)
  - Politische Micro-Targeting-Systeme
- Erfordert Risikomanagement, Qualitätskontrollen, Dokumentationspflichten und menschliche Aufsicht.

❌ 4. Unannehmbares Risiko (Verboten)

- Beispiele:
  - Sozialkreditsysteme nach chinesischem Vorbild
  - Biometrische Echtzeit-Überwachung im öffentlichen Raum (z.B. Gesichtserkennung)
  - KI, die Menschen gezielt manipuliert oder schadet (z.B. Spielzeug mit versteckter Manipulation von Kindern)
- Komplettes Einsatzverbot in der EU.

DETAIL:
Der EU AI Act verfolgt einen risikobasierten Ansatz zur Regulierung von Künstlicher Intelligenz (KI) und unterteilt KI-Systeme in vier Risikokategorien:

1. Unannehmbares Risiko – Verbotene KI-Systeme
Diese KI-Systeme sind aufgrund ihrer potenziellen Gefährdung für Sicherheit, Grundrechte und demokratische Werte verboten. Beispiele umfassen:
Manipulative KI, die menschliches Verhalten subliminal beeinflusst.
Ausnutzung von Schwächen bestimmter Gruppen (z. B. Kinder, Menschen mit Behinderungen).
Soziale Bewertungssysteme (Social Scoring) durch Behörden.
Echtzeit-Biometrie in öffentlichen Räumen zur Strafverfolgung (mit wenigen Ausnahmen).(Wikipedia, EU Artificial Intelligence Act)
Diese Systeme dürfen in der EU weder in Verkehr gebracht noch betrieben werden.

2. Hohes Risiko – Streng regulierte KI-Systeme
KI-Systeme gelten als hochriskant, wenn sie:(EU Artificial Intelligence Act)
Als Sicherheitskomponente eines Produkts dienen, das unter EU-Harmonisierungsgesetze fällt (z. B. Medizinprodukte, Fahrzeuge).
In Bereichen wie kritischer Infrastruktur, Bildung, Beschäftigung, Zugang zu wesentlichen Dienstleistungen, Strafverfolgung, Migration oder Justiz eingesetzt werden.(wilmerhale.com, Pinsent Masons)
Solche Systeme unterliegen strengen Anforderungen, einschließlich Risikomanagement, Datenqualität, Transparenz, menschlicher Aufsicht und Konformitätsbewertung.(Wikipedia)

3. Geringes Risiko – Transparenzpflichtige KI-Systeme
Diese Systeme erfordern spezifische Transparenzmaßnahmen, wie die Information der Nutzer über die Interaktion mit einer KI. Beispiele sind:

- Chatbots.
- Deepfake-Technologien
- KI-generierte Inhalte.(The Guardian, Europäisches Parlament)

Ziel ist es, die Nutzer in die Lage zu versetzen, informierte Entscheidungen zu treffen.

4. Minimales Risiko – Nicht regulierte KI-Systeme
Die Mehrheit der KI-Anwendungen fällt in diese Kategorie, darunter:

- Spam-Filter.
- Videospiele.
- Empfehlungssysteme für Musik oder Filme.(trail-ml.com)

Für diese Systeme bestehen keine spezifischen gesetzlichen Verpflichtungen, jedoch wird die Einhaltung freiwilliger Verhaltenskodizes empfohlen.

Sonderkategorie: Allgemeine KI (General Purpose AI, GPAI)
Für GPAI-Modelle gelten zusätzliche Anforderungen:(EU Artificial Intelligence Act)

- Bereitstellung technischer Dokumentation und Nutzungsanleitungen.
- Einhaltung des Urheberrechts.

- Veröffentlichung einer Zusammenfassung der für das Training verwendeten Inhalte.(EU Artificial Intelligence Act)
- Modelle mit systemischem Risiko müssen zudem Modellbewertungen durchführen, adversarielle Tests bestehen, schwerwiegende Vorfälle melden und Cybersicherheitsmaßnahmen implementieren.(EU Artificial Intelligence Act)

Diese Klassifizierung ermöglicht es, KI-Systeme entsprechend ihrem Risikopotenzial zu regulieren und so Sicherheit, Transparenz und den Schutz der Grundrechte zu gewährleisten.