KI-TRANSPARENZBERICHT NEOS - Das Neue Österreich und Liberales Forum Landesgruppe OÖ & NEOS Landtagsklub OÖ

Berichtszeitraum: 01.01.2025 – 02.06.2025

Veröffentlichungsdatum: 02.06.2025

1. Einleitung

Im Sinne unserer ethischen Standards, unserer Verantwortung für die gemeinsame politische Debatte und unseres Transparenzversprechens der an die Oberösterreicher:innen legen wir mit diesem Bericht offen, wie wir KI-Werkzeuge in der politischen Arbeit einsetzen.

Ziel ist es, Transparenz zu schaffen, Vertrauen zu stärken und kontinuierliche Verbesserung zu ermöglichen.

2. Unsere Grundsätze

Wir setzen KI-Werkzeuge ausschließlich nach den folgenden Grundsätzen ein:

- Menschliche Verantwortung: Die Verantwortung trägt immer der Mensch, nie die Maschine.
- Kennzeichnung: Wir kennzeichnen KI-generierte audiovisuelle Inhalte als solche.
- Gesetzeskonformität: Wir achten stets auf die Einhaltung des EU AI Act und der DSGVO.
- Manipulationsverzicht: Wir verzichten auf manipulative, KI-generierte Inhalte.

3. Verwendete KI-Werkzeuge im Berichtszeitraum

Berichtszeitraum: 01-05 2025			
Tool / Anbieter	**Zweck / Einsatzgebiet**	**Risiko-Klassifizierung (EU AI Act)**	**Kennzeichnung**
ChatGPT / OpenAI]	Unterstützung bei der Textgenerierung	Minimales Risiko	nicht erforderlich
	Audio- und Videoinhalte	Geringes Risiko	JA
	Interne Analysen	Geringes Risiko	JA (intern)
	Social Media Postings	Minimales Risiko	nicht erforderlich
Canva Magic Write/ & Expand	Social Media Postings	Minimales Risiko	nicht erforderlich
General Purpose AI -GPAI (NEOS-Test)	Analyse, Strategie	Sonderregelungen	Training intern

4. Konkrete Anwendungsfälle

4.1 Beschreibung der Einsätze

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

4.2 Kennzeichnung

- Bisher keine audiovisuellen Inhalte, die mit KI erstellt wurden

5. Evaluierung der KI-Einsätze

5.1 Erkenntnisse

- Zusammenfassen von LRH Berichten - Hauptanwendungsfall, rein für den internen Gebrauch in nicht öffentlichen Ausschusssitzungen
- Strukturieren von Themenfeldern zur Vorbereitung von Landtagssitzungen
- Anträge/ Anfragen: gar nicht, hier empfinden wir KI leider als überhaupt nicht sinnvoll

5.2 Positivbeispiele

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

5.3 Verbesserungspotenziale

- Sensibilisierung des Teams für die Prüfung von Inhalten
- Werden künftig 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 der KI-Kompetenz des Teams durch gezielte Schulungen

7. Fortbildungen und Sensibilisierungen

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

8. Ausblick

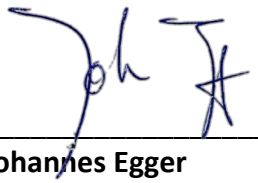
Das Thema KI wird weiterhin Bestandteil regelmäßiger Teammeetings und Fortbildungen sein.

9. Impressum / Kontakt

Herausgeber: NEOS Landesgruppe OÖ
Verantwortlich: Johannes Egger
Kontakt: johannes.egger@neos.eu
Webseite: https://oberoesterreich.neos.eu

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

Felix Eypeltauer
Klubobmann, Landessprecher NEOS OÖ



Johannes Egger
Landesgeschäftsführer NEOS OÖ

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 (müssen als solche gekennzeichnet 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.