K-01

Verwendung Künstlicher Intelligenz bei BÜNDNIS 90/DIE GRÜNEN

1. Ordentlicher Länderrat 2026
Sassnitz, 28. Juni 2026

Gremium:	Bundesvorstand
Beschlussdatum:	08.06.2026
Tagesordnungspunkt:	K KI-Strategie

Antragstext

Künstliche Intelligenz ist die größte technologische Veränderung seit der industriellen Revolution. Sie verändert die Arbeit in nahezu allen Betrieben, Behörden und Organisationen. Auch in unserer Partei wird KI an vielen Stellen bereits genutzt, in der Regel jedoch außerhalb geregelter Prozesse und ohne gemeinsame Standards. Diese Realität anzuerkennen ist die Voraussetzung dafür, sie aktiv zu gestalten.

BÜNDNIS 90/DIE GRÜNEN haben sich als Partei nie davor gescheut, technologische Umbrüche anzunehmen und sie zum Maßstab grüner Werte zu machen. Genau diesen Anspruch lösen wir auch in unserer eigenen Organisation ein. Den Möglichkeiten von KI verschlossen zu bleiben, wäre fahrlässig. Sie unreflektiert zu übernehmen, wäre unklug. Wir wählen einen dritten Weg: Wir nutzen KI souverän, gestalten den Einsatz selbstbestimmt und richten ihn an unseren Werten aus: an Demokratie, digitaler Souveränität, Datenschutz, Transparenz, Nachhaltigkeit, Teilhabe, Gemeinwohlorientierung, Barrierefreiheit, Fairness und einem verantwortungsvollen, diskriminierungsfreien Umgang mit Technologie. KI soll Menschen unterstützen, nicht ersetzen, demokratische Prozesse stärken statt manipulieren und offen, nachvollziehbar sowie im Sinne des Gemeinwohls eingesetzt werden. Dabei achten wir auf Datensparsamkeit, ökologische Verantwortung, offene Standards und eine starke europäische digitale Infrastruktur.

Die politische Arbeit unserer Partei ist text-, daten- und kommunikationsintensiv. Das gilt für die strategisch-inhaltliche Arbeit ebenso wie für Kommunikation, Mitgliederbetreuung, Wahlkampforganisation, Veranstaltungs- und Wissensmanagement und die Verwaltung. Genau dort entfaltet KI heute ihren größten Nutzen. Sie beschleunigt Recherche und Synthese, bereitet Entwürfe vor, automatisiert Routinen, übersetzt, strukturiert große Mengen an Eingaben und entlastet Mitarbeitende von kleinteiliger Arbeit. So wird Zeit frei für das, was nur Menschen können: politisches Urteil, Beziehungsarbeit, Gestaltung.

Die technische Landschaft ist im dauerhaften Wandel. Modelle, Anbieter und Risiken verändern sich in Wochen, nicht in Jahren. Der Bundesverband beobachtet die Entwicklung eng, aktualisiert sowohl die offenen als auch die kommerziellen Modelle gemäß einer transparenten Priorisierung und passt Ausschluss- und Anbieterlisten regelmäßig an.

Der Umgang mit KI wird damit zu einer dauerhaften organisatorischen Aufgabe, die Austausch, Weiterbildung, Anpassungsfähigkeit und kontinuierliche Weiterentwicklung voraussetzt. Mit der Weiterentwicklung von KI-Systemen verändern sich auch mögliche Sicherheitsrisiken fortlaufend, sowohl bei Open-Source-Modellen als auch bei kommerziellen Anwendungen. Neue Systeme können zusätzliche Angriffsflächen schaffen oder missbräuchliche Nutzungen erleichtern. Deshalb müssen technische, organisatorische und rechtliche Risiken kontinuierlich beobachtet, bewertet und an neue Entwicklungen angepasst werden. Sicherheitsprüfung ist damit keine einmalige Aufgabe, sondern ein fortlaufender Prozess.

Gemeinsame Handlungsempfehlungen werden daher nie abgeschlossen sein, sondern legen einen gemeinsamen Entwicklungsprozess, Anwendungen, Regelungen und Verfahren fest, die regelmäßig evaluiert werden. Erfahrungen aus der Praxis werden aufgenommen und neue Erkenntnisse systematisch berücksichtigt. Ziel ist es, schrittweise tragfähige Standards aufzubauen, aus der Nutzung zu lernen und auf Veränderungen handlungsfähig reagieren zu können.

Beschluss

Der Bundesverband und die Landesverbände erarbeiten im Rahmen einer gemeinsamen Digitalstrategie Handlungsempfehlungen für den Einsatz von KI in der politischen Arbeit.

Folgende Prinzipien sollen dafür leitend sein:

1. **Souveränität**

Der Einsatz von KI im Bundesverband folgt dem Grundsatz digitaler Souveränität, wie ihn die 51. Bundesdelegiertenkonferenz in Hannover (November 2025) im Beschluss „Digitale Souveränität stärken" festgehalten hat. Wir wollen frei entscheiden können, welche Technologien wir einsetzen, auf welcher Infrastruktur sie laufen und welche Daten sie verarbeiten. Wir vermeiden neue Abhängigkeiten und bauen bestehende ab. Was aus Mitgliedsbeiträgen finanziert wird, soll der Partei und ihren Strukturen langfristig zugutekommen.

2. **Self-Hosted KI-Interfaces als Standard**

Eingesetzt werden selbst betriebene, auf Open Source basierende KI-Interfaces. Sie laufen auf souverän kontrollierter Infrastruktur, lokal oder bei einem europäischen Auftragsverarbeiter, und greifen in der Standardkonfiguration auf offene, frei verfügbare Modelle zurück.

Wo Anwendungsfälle die Fähigkeiten offener Modelle erkennbar überschreiten, kann das interne Interface um geprüfte kommerzielle Modelle europäischer Anbieter erweitert werden. In zu begründenden Ausnahmefällen können geprüfte kommerzielle KI-Plattformen auch direkt und außerhalb der eigenen Sandbox genutzt werden. Das betrifft Anwendungsfälle, in denen plattformspezifische Funktionen erforderlich sind, die sich technisch nicht über die eigene Schnittstelle abbilden lassen, etwa fortgeschrittene multimodale Werkzeuge, spezialisierte Recherche- und Analysefunktionen oder die Zusammenarbeit mit externen Partner*innen auf einer gemeinsamen Plattform.

Die direkte Nutzung kommerzieller Modelle ist die Ausnahme, nicht die Regel. Für sie gelten zusätzliche Auflagen.

Wahrung von Urheber- und Leistungsschutzrechten. Der KI-Einsatz respektiert geistiges Eigentum. Inhalte werden nicht ohne Berechtigung verarbeitet oder reproduziert, fremde Werke werden nicht ungekennzeichnet übernommen. Bei der Auswahl von Modellen werden Anbieter bevorzugt, die ihre Trainingsdaten transparent machen und Urheber*innen angemessen beteiligen.

Ausschluss von Diskriminierung. KI-Systeme dürfen nicht eingesetzt werden, wo sie Diskriminierung erzeugen oder verfestigen. Modelle und Anwendungen werden auf Verzerrungen geprüft, insbesondere auf rassistische, sexistische, antisemitische, queerfeindliche oder behindertenfeindliche Muster. Auffällige Modelle werden nicht eingesetzt.

Barrierefreiheit. KI-Werkzeuge in der BGSt werden so ausgewählt und konfiguriert, dass sie für Mitarbeitende mit Behinderungen zugänglich sind. Barrierefreiheit nach den geltenden Standards (BITV, WCAG) ist verbindliches Auswahlkriterium. Wo KI-Werkzeuge Barrieren senken können, etwa bei Texterstellung, Übersetzung oder Bildbeschreibung, werden sie aktiv dafür eingesetzt.

3. **Transparenz**

Wesentlich KI-erstellte Inhalte werden, wo es für Empfänger*innen oder die Öffentlichkeit relevant ist, gekennzeichnet.

4. **Beschaffungsregeln**

Politisch oder ideologisch manipulierte KI-Modelle sind ausgeschlossen und die Liste der empfohlenen KI-Modelle wird regelmäßig überprüft. KI wird DSGVO- und AI-Act-konform eingesetzt; Anwendungen, die in die Rechte von Mitarbeitenden oder Mitgliedern eingreifen, sind ausgeschlossen. In der Beschaffung gilt „Open Source first“, offene Standards und die Vermeidung von Abhängigkeiten. Energie- und Ressourceneffizienz sind verbindliche Auswahlkriterien. Europäische Anbieter werden bevorzugt; Ausnahmen müssen begründet und dokumentiert werden.

5. **Weiterbildung**

Bundesverband und Landesverbände bauen für Anwendungsfälle, Schulungen, Sicherheits- und Datenschutzfragen eine Unterstützungsstruktur auf.

Begründung

I. Politische Anschlussfähigkeit

Der Beschluss ist die innerorganisatorische Übersetzung dreier programmatischer Linien:

- des BDK-Beschlusses „Digitale Souveränität stärken" (51. BDK Hannover, 28.–30.11.2025), der digitale Selbstbestimmung, Open Source, sichere Cloud-Infrastrukturen und den Abbau bestehender Abhängigkeiten zum politischen Leitprinzip macht;
- der Linie der Bundestagsfraktion zu „KI made in Europe" und zur Umsetzung der KI-Verordnung (Anträge 21/2349 „Vertrauenswürdige Künstliche Intelligenz ermöglichen" und 21/2726 „Strategie zur Digitalen Souveränität"), in denen Open Source ausdrücklich als Pfad „transparenter, nachhaltiger und souveräner KI-Systeme" beschrieben wird;
- bündnisgrüne Beschlüsse auf Landesebene, etwa der Open-Source-Strategie des Freistaates Sachsen unter bündnisgrüner Mitwirkung (2022) und des Forderungspapiers GRÜNE NRW (2024), die den Grundsatz „öffentliches Geld – öffentliches Gut" in konkrete Verwaltungs- und Beschaffungslogik übersetzen.

Der Ausschluss von Modellen mit manipulierten Trainingsdaten oder manipulierter Inferenz ist nicht nur grüne Position, sondern entspricht inzwischen auch der Risikoeinschätzung der Konferenz der Regierungschefinnen und Regierungschefs der Länder vom 12. März 2025, die proprietäre Systeme ohne vollen Quellcode-Zugriff als „erhebliches Risiko für die IT-Sicherheit kritischer Infrastrukturen und sicherheitsrelevanter KI-Anwendungen" bezeichnet hat.

II. Gestaffelter Hybrid-Ansatz als Standard

Ein „nur Open Source"-Modell wäre politisch attraktiv, ist aber operativ nicht in jedem Anwendungsfall ausreichend. Ein „nur kommerzielles" Modell wäre einfach beschaffbar, aber souveränitäts- und datenschutzpolitisch nicht politisch vertretbar und im Übrigen nicht im Einklang mit unserer bisherigen Beschlusslage. Der Hybrid-Ansatz antwortet auf diesen Konflikt: Er nutzt Open Source als Standard und Rückgrat, lässt aber kontrollierten Zugriff auf kommerzielle Modelle dort zu, wo Anwendungsfälle es erfordern. Bevorzugt über ein eigenes, kontrolliertes Interface, mit klaren Verträgen, ohne Datenabfluss zu Trainingszwecken und mit einer dokumentierten Auswahllogik.

Handlungsfähigkeit bei asymmetrischer Bedrohung

Wir gehen davon aus, dass nicht alle Akteure im politischen Raum vergleichbare Selbstbeschränkungen anlegen. KI-gestützte Angriffe, koordinierte Desinformation und der Missbrauch leistungsfähiger Modelle durch politische Gegner oder ausländische Akteure können unsere Cybersicht massiv beeinträchtigen.

Bei einer konkreten, sicherheitsrelevanten Bedrohung dürfen zum Erkennen, Abwehren oder Aufklären einer Bedrohung deshalb vorübergehend auch leistungsfähigere kommerzielle Modelle eingesetzt werden, einschließlich möglicherweise nicht öffentlich verfügbarer oder nur eingeschränkt zugänglicher Modelle. Ziel ist mindestens technische Parität zu denjenigen, die uns angreifen oder zu manipulieren versuchen.

III. Wirkung gegen Schatten-KI

Erfahrungen aus Verwaltung und Unternehmen zeigen: Ohne ein internes Angebot von vergleichbarer Qualität und klare Leitlinie nutzen Mitarbeitende private Accounts kommerzieller Anbieter („Shadow KI"). Damit fließen Informationen unkontrolliert ab und Risiken werden privatisiert. Ein gutes internes Werkzeug ist die wirksamste Maßnahme gegen diese Praxis – stärker als jedes Verbot. Die kombinierte Strategie aus „besser als die Free-Versionen" und einem klaren Verbot der Free-Versionen ist wirksam, weil sie kein Werkzeug verbietet, ohne ein besseres bereitzustellen.