Kompetenzzentrum Öffentliche IT

Forschung für den digitalen Staat

Dorian Wachsmann, Gabriele Goldacker, Hannes Hartmann, Nicole Opiela, Chris Schmitz, Mike Weber, Christian Weidner

Digitale Souveränität und grosse Sprachmodelle in der Bundesverwaltung

Gefördert durch:

Bundesministerium des Innern

aufgrund eines Beschlusses des Deutschen Bundestages

Fraunhofer FOKUS

Impressum

Die Marktbetrachtung, die Analyse der Strategien sowie die Datenerhebung und -Auswertung wurden Anfang 2025 durchgeführt. Für die Handlungsempfehlungen wurden Entwicklungen bis Sommer 2025 berücksichtigt.

Teile der Studie wurden mit Unterstützung generativer Künstlicher Intelligenz erstellt. Diese wurde genutzt:

- Bei der Recherche relevanter Literatur (Deep Research)
- Für die sprachliche Finalisierung ausgewählter ausgearbeiteter Inhalte

Autor:innen:
Dorian Wachsmann, Gabriele Goldacker, Hannes Hartmann, Nicole Opiela, Chris Schmitz, Mike Weber, Christian Weidner

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

ISBN: 978-3-948582-33-3

1. Auflage November 2025

Icons für Infografik: https://fontawesome.com/

Das letzte Abrufdatum der Onlinequellen ist der 24.11.2025.

Bildnachweis

Seite 1:	susnpics	https://pixabay.com/de/
Seite 6:	Tom6667	https://pixabay.com/de/
Seite 16	XtianDuGard	https://pixabay.com/de/
Seite 24	Keishpixl	https://pixabay.com/de/
Seite 35	kudybadorota	https://pixabay.com/de/
Seite 47	raksasokh	https://pixabay.com/de/

Vorwort

Auf eigenen Beinen stehen, sich selbständig, selbstbestimmt und sicher – kurz: souverän – in der Welt bewegen zu können, ist ein wohl entscheidender Schritt im Erwachsenwerden. Doch auch wenn eine große Handlungsautonomie erreicht wird, ist damit keineswegs gesichert, dass sie auch Bestand hat. Von Lebensrisiken über freiwillige Selbstbindungen bis hin zur wahrscheinlichen Hilfsbedürftigkeit im Alter stellen sich immer neue Herausforderungen. Diesen angemessen zu begegnen, bestimmt wesentlich darüber, wie souverän der Alltag gemeistert wird.

Was für Menschen gilt, lässt sich auch auf Staaten und Volkswirtschaften übertragen. Um Handlungsautonomie langfristig zu wahren, müssen die Herausforderungen für die Souveränität frühzeitig erkannt und adressiert werden. Dies umso mehr, wenn sicher geglaubte Rahmenbedingungen durch Kriege, politische Neuausrichtungen und Lieferkettenprobleme zu erodieren drohen.

Im Bereich des Digitalen konnte Deutschland in der Vergangenheit oft genug seine Souveränität nicht im erwünschten Umfang wahren. Zu den bereits nachgewiesenen Abhängigkeiten in den Bereichen der Bürosoftware und Datenbanken ließen sich bei breiterer Analyse wohl noch weitere Felder finden, in denen sich der deutsche Staat in direkter Abhängigkeit von wenigen ausländischen Unternehmen befindet.

So unbefriedigend die Situation punktuell zu sein scheint, so dynamisch verändert sich die digitale Welt. Dominante Akteure auf den zentralen Märkten können nach dem nächsten Paradigmenwechsel erheblich an Einfluss verlieren, es können aber auch neue Abhängigkeiten von denselben oder anderen Akteuren entstehen. Mit generativer KI durchleben wir gerade einen solchen Paradigmenwechsel, der die Karten neu verteilt. Umso wichtiger ist es, gerade jetzt einen vertieften Blick auf die aktuellen Entwicklungen im Bereich der für die öffentliche Verwaltung besonders wichtigen großen Sprachmodelle zu werfen. Denn jetzt entscheidet sich, ob Deutschland den nächsten Innovationszyklus souverän durchschreiten und möglicherweise sogar mitgestalten kann oder ob ein langfristiger Verlust an Handlungsfähigkeit droht.

Einige konzeptionelle und empirische Antworten zur Frage, wie die Bundesverwaltung in ihren Rollen als Bereitsteller, Entwickler und Auftraggeber bezogen auf Anwendungen großer Sprachmodelle bei der Erfüllung der strategischen Souveränitätsziele *Wechselmöglichkeit*, *Gestaltungsfähigkeit* und *Einfluss auf Anbieter* aufgestellt ist, finden Sie in dieser Studie, die mit umfassenden Handlungsempfehlungen schließt, die zeitlich und inhaltlich über den Rahmen Studie hinausblicken.

Wir wünschen eine inspirierende Lektüre.

Ihr Kompetenzzentrum Öffentliche IT

Inhalt

Das Wichtigste in Kürze

Diese Studie betrachtet digitale Souveränität im Kontext großer Sprachmodelle (LLMs) in der Bundesverwaltung durch die Analyse der derzeitigen (Eigen-)Entwicklungen. Somit wird auf einen klar durch die entwickelten Lösungen definierten Bereich generativer KI fokussiert. Dazu wurde eine Datenerhebung mit relevanten Projekten durchgeführt, um diese mit Fokus auf die drei Souveränitätsziele *Wechselmöglichkeit*, *Gestaltungsfähigkeit* und *Einfluss auf Anbieter* entlang einer entwickelten Indikatorik (siehe Anhang A.5) einzuschätzen und darüber hinausführende Handlungsempfehlungen (siehe Abschnitt 8) abzuleiten. Als Basis dafür wurde zuerst eine Marktbetrachtung zu LLMs sowie eine Analyse der Maßnahmen zur digitalen Souveränität in Bezug auf KI und LLMs in Deutschland und in ausgewählten weiteren Ländern durchgeführt.

Die zentralen Erkenntnisse dieser Studie sind:

1. Durch die Eigenentwicklungen der Bundesverwaltung von technischen Systemen mit großen Sprachmodellen (LLMs) muss für viele der LLM-typischen Anwendungsfälle nicht auf Produkte von (vor allem nicht-europäischen) Großkonzernen zurückgegriffen werden. So werden Risiken vermindert, sich in neue Abhängigkeiten zu Technologieanbietern begeben zu müssen beziehungsweise bestehende Abhängigkeiten zu vertiefen.
2. Die entwickelten Lösungen dienen derzeit ausschließlich als Arbeitsunterstützung für die Verwaltungsmitarbeitenden, sodass ein Ausfall die Handlungsfähigkeit der Verwaltungen nicht bedrohen würde. Die Risiken für die digitale Souveränität sind aus dieser Perspektive daher überschaubar. Große Systeme, die ressortübergreifend angeboten werden und damit potenziell einer großen Nutzer:innenbasis zur Verfügung stehen, werden außerdem nach Kriterien entwickelt, welche digitale Souveränität berücksichtigen. Die Gefahr erscheint gering, sich hier in eine Situation der Erpressbarkeit oder Handlungsunfähigkeit zu begeben. Das liegt daran, dass (a) die LLMs zumeist auf eigener Hardware laufen, sie (b) bei Bedarf mit geringem bis mittlerem Aufwand ausgetauscht werden können oder mehrere hinreichend leistungsstarke Modelle zur Auswahl stehen und (c) keine externen Anbieter wesentlich zum Betrieb oder der Weiterentwicklung der Anwendung nötig sind.
3. Auf Ebene der LLMs wird hauptsächlich auf nicht-europäische Open-Source-Lösungen gesetzt, die auf verwaltungsinterner Hardware gehostet sind. Vor dem Hintergrund eines sich wandelnden Open-Source-Verständnisses im Kontext von KI und zur Sicherstellung der Berücksichtigung von verwaltungsspezifischen Anforderungen ist die Entwicklung eines eigenen, auf europäische Normen und Werte ausgerichteten und offen bereitgestellten LLMs zu evaluieren und ggf. anzustreben. Ziel sollte sein, eine dauerhafte Unabhängigkeit von marktbeherrschenden LLM-Anbietern zu erreichen und die Leistungsfähigkeit der europäischen KI-Landschaft zu präsentieren (siehe auch Handlungsempfehlung 8.2.1).

Darüber hinaus ergab die Metaanalyse von Marktstudien zu LLMs (siehe Abschnitt 3): Anwendungen mit LLMs in der Domäne »staatlicher Sektor« sind derzeit ein Nischenmarkt. Hier stellt sich die Frage, ob die Entstehung eines Ökosystems rund um Anwendungen mit LLMs durch Investitionen, Förderanreize, gezielte Beschaffungsmaßnahmen und Kooperation angeregt werden sollte oder ob die Eigenentwicklungen ausreichen, wenn diese auch über föderale Grenzen hinweg bereitgestellt werden können, wie es derzeit im Rahmen des Deutschland-Stacks diskutiert wird.

Die Analyse der Eigenentwicklungen der Bundesverwaltung hat einige Herausforderungen aufgedeckt, mit denen sich die Projekte konfrontiert sehen (siehe auch Abschnitt 6.4). Dazu gehören u. a. als zu kompliziert wahrgenommene rechtliche KI-Regelungen, welche Entwicklungen verzögern und umfassende rechtliche Kompetenzen nötig machen. Rechtliche Unsicherheiten führen dann auch zu einer geringeren Bereitstellung zur Nachnutzung. Schließlich wurde mehrfach KI-spezifische Cloud-Infrastruktur gewünscht, gekoppelt mit entsprechend geschultem Personal mit KI-Kompetenz.

Festzuhalten bleibt, dass die gegenwärtigen LLM-Projekte im Bund in ihren Bereichen praktikable Alternativen zu externen Anbietern darstellen und somit die digitale Souveränität stärken. Gleichwohl zeigen sich Schwächen, unter anderem auf der Betrachtungsebene der LLMs, es bedarf also zielgerichteter Handlung, um bestehende Abhängigkeiten nicht zu vertiefen und in Zukunft nicht in neue Abhängigkeiten zu geraten. Dazu werden in Abschnitt 8 Handlungsempfehlungen strukturiert nach den vier Clustern »gemeinsame Infrastruktur«, »Open Source«, »rechtliche Vorgaben« und »weitere Maßnahmen« gemacht.

1. Gegenstand der Studie

Digitale Souveränität ist nicht erst durch die jüngsten geopolitischen Veränderungen in den öffentlichen Fokus gerückt, sondern »hat sich in den letzten Jahren zu einem neuen Schlüsselbegriff der deutschen und europäischen Digitalpolitik entwickelt« (Steer und Pohle 2024). Und das aus gutem Grund: Bei der Versorgung mit IT-Hardware und digitalen Dienstleistungen ist die Exportnation Deutschland massiv auf Importe angewiesen. Entsprechend schätzen auch Unternehmen laut einer von dem Bitkom durchgeführten Befragung ihre Abhängigkeit vom Import bei digitalen Technologien als hoch ein, wobei die Abhängigkeit bei Halbleitern als besonders hoch (49 Prozent stark abhängig und 34 Prozent eher abhängig), bei Künstlicher Intelligenz als noch als vergleichsweise hoch (20 Prozent und 47 Prozent) und bei Robotik als vergleichsweise gering (9 Prozent und 37 Prozent) eingeschätzt wird. Für die nähere Zukunft wird mit einer wachsenden Abhängigkeit im Bereich der digitalen Technologien gerechnet (Bitkom 2025, 12 f.).

Auch für Staat und Verwaltung ergeben sich aus solchen Abhängigkeiten Schmerzpunkte und Risiken, wie Untersuchungen zu den Themenfeldern Bürosoftware (PwC 2019) und Datenbankprodukte (Deloitte 2021) gezeigt haben. Abhängigkeiten können potenziell ausgenutzt werden und Handlungsmöglichkeiten einschränken, die dann wiederum zu Schmerzpunkten bei den Betroffenen führen können. Die Schmerzpunkte können gleichermaßen ökonomische, betriebliche, technische und rechtliche Aspekte betreffen und die Handlungsfähigkeit von Staat und Verwaltung über den Bereich der Digitalpolitik hinaus beeinflussen.

Digitale Souveränität ist in einer sich verändernden Welt kein Zustand, welcher, einmal erreicht, als dann für immer gegeben angesehen werden kann. Vielmehr lässt sich digitale Souveränität als mehrdimensionales Zielbild verstehen. Dabei lassen sich Abhängigkeiten bei für die IT typischen, hoch komplexen Systemen nicht immer vermeiden. Vielmehr geht es um die Analyse dieser Abhängigkeiten, der Identifikation der sich daraus möglicherweise ergebenden Schmerzpunkte und die Ableitung von Handlungsmöglichkeiten, diese Abhängigkeiten so zu managen, dass daraus keine zu starken Einschränkungen der Handlungsfähigkeit des Staates entstehen. Das Ziel eines souveränen Staates muss somit eine strategische Autonomie unter Nutzung möglichst vielfältiger Instrumente – beginnend mit der Analyse des Ist-Zustandes über gezielte Netzwerkarbeit in relevanten Ökosystemen bis hin zu technischen, organisatorischen und rechtlichen Abwehrmaßnahmen – sein (Mohabbat Kar und Thapa 2020).

Diese Studie nimmt ein Technologiefeld in den Blick, das aktuell sowohl hinsichtlich seiner wirtschaftlichen und gesellschaftlichen Wirkungen als auch hinsichtlich seiner potenziell überragenden Bedeutung für den öffentlichen Sektor intensiv diskutiert wird: Künstliche Intelligenz. Jenseits seit Jahrzehnten wiederkehrender Heilsversprechen und Untergangsdystopien eröffnen die hoch dynamischen Entwicklungen der letzten Jahre, insbesondere im Bereich der großen Sprachmodelle, neue Anwendungsfelder gerade auch im öffentlichen Sektor. Dies zeigt sich bereits in der Praxis. Eine europaweite Befragung (Fontana et al. 2024, S. 54) ergab, dass auch auf regionaler und lokaler Ebene etwa 27 Prozent der auf die Befragung antwortenden Verwaltungen bereits KI-Anwendungen einsetzen. Auf gesamtstaatlicher Ebene fällt der Anteil noch höher aus (ebd.). Noch befinden sich viele KI-Anwendungen in der Entwicklungs-, Evaluations- oder Testphase und übernehmen wenig kritische Aufgaben in den öffentlichen Verwaltungen. Bei weiterhin dynamischer Entwicklung wird sich dies jedoch aller Voraussicht nach, etwa durch die flächendeckende Anwendung, absehbar ändern und damit Fragen nach der digitalen Souveränität in diesem Bereich virulenter werden lassen.

Dabei richtet sich die öffentliche Aufmerksamkeit aktuell stark auf Fortschritte von US-amerikanischen und mitunter auch chinesischen großen Sprachmodellen. Wachsende Bedeutung und immer breitere Anwendungsfelder in der öffentlichen Verwaltung auf der einen und Dominanz außereuropäischer Technologieanbieter auf der anderen Seite werfen die Frage auf, ob Deutschland Gefahr läuft, sich in diesem Technologiefeld in ähnliche Abhängigkeiten zu begeben, wie es für Bürosoftware und Datenbankprodukte bereits festgestellt wurde (siehe (PwC 2019) und (Deloitte 2021)).

Diese Studie fokussiert auf die Verwendung großer Sprachmodelle in Projekten des Bundes, konkret wird geprüft, ob bereits kritische Abhängigkeiten im Bereich LLMs der Bundesverwaltung existieren. Sofern dies der Fall ist, sollen Handlungsempfehlungen ausgearbeitet werden, die helfen, diese Abhängigkeiten zu reduzieren. Sollten im Rahmen der Studie keine kritischen Abhängigkeiten identifiziert werden, so ist das Ziel der Studie, Handlungsempfehlungen abzuleiten, die diesen Zustand erhalten. So sollen die Handlungs- und Entscheidungsspielräume ausgelotet und erweitert werden. Dazu ist es erforderlich, auch die Systeme zu betrachten, in die große Sprachmodelle eingebettet sind.

Das dazu erforderliche empirische Lagebild speist sich aus vier Quellen. Das sind (1) eine nicht verwaltungsspezifische Betrachtung des KI-Marktes mit Fokus auf große Sprachmodelle und Open Source (Abschnitt 3), außerdem (2) eine Übersicht über den aktuellen Stand der Umsetzung von Souveränitätsmaßnahmen bezogen auf KI (Abschnitt 4 und Abschnitt 5), (3) eine quantitative Erhebung von Projekten mit LLM-Einsatz in der Bundesverwaltung (Abschnitt 6) sowie ergänzend (4) Interviews mit relevanten Stakeholdern – insbesondere Projektmitarbeitenden – aus der öffentlichen Verwaltung in Deutschland.

Daraus ergeben sich zugleich die Limitationen und Restriktionen der hier durchgeführten Untersuchung. Die Studie nimmt nicht die gesamte Nutzung von generativer KI in den Blick. So lässt sich empirische Evidenz dafür finden, dass die Mitarbeitenden in den öffentlichen Verwaltungen auch Tools für ihre Arbeit verwenden, die nicht von den Behördenleitungen bereitgestellt werden (Wachsmann und Weber 2025, S. 13). Auch bleibt die Betrachtung des Technologie-Stacks notwendig beschränkt, um weder den Rahmen der Untersuchung zu sprengen, noch den Fokus der Studie zu verschieben. So werden explizit keine Bewertungen der Cloud-Infrastruktur vorgenommen, für die eine KI-unspezifische Betrachtung ganz eigener Souveränitätsanforderungen erforderlich wäre.

Die nächsten Abschnitte setzen sich zunächst mit den hier verwendeten Konzepten von digitaler Souveränität sowie mit dem aktuellen Stand der Entwicklung von KI auseinander.

1.1 Digitale Souveränität

Digitale Souveränität bedeutet, sich selbstständig, selbstbestimmt und sicher in der digitalen Welt bewegen zu können (Goldacker 2017, S. 3). Die zentrale strategische Basis für die Betrachtung und die Umsetzung digitaler Souveränität in der deutschen öffentlichen Verwaltung ist die »Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung« des IT-Planungsrates (IT-Planungsrat 2021). Sie ordnet jede der sieben, von Mohabbat Kar und Thapa (2020, S. 13–15) vorgeschlagenen Souveränitätsdimensionen Wissenssouveränität, Forschungssouveränität, Entwicklungssouveränität, Produktionssouveränität, Betriebssouveränität, Nutzungssouveränität und Transparenzsouveränität der institutionellen Rolle derer zu, bei denen die jeweilige Dimension ihren praktischen Einfluss besonders stark entfaltet, und leitet daraus drei strategische Ziele ab.

Auf der Ebene der (institutionellen) Nutzer:innen, also der einsetzenden Behörden, Ämter und Einrichtungen, müssen nach innen (also vor allem für die individuell nutzenden Behördenmitarbeitenden) Voraussetzungen für eine erfolgreiche, effiziente und (rechts)sichere Nutzung (Nutzungssouveränität) digitaler Technologien geschaffen werden. Dazu gehören Auswahl- sowie flexible Wechsel- und Konfigurationsmöglichkeiten für die Institution oder sogar die individuell Nutzenden. Das strategische Ziel lautet hier kurz: *Wechselmöglichkeit*. Es umfasst im Wesentlichen zwei unterschiedliche Aspekte: einerseits die faktische Verfügbarkeit akzeptabler Alternativen für Systemkomponenten – hier vor allem für das bzw. die eingesetzten großen Sprachmodelle – bzw. Systeme und andererseits die adäquate Gestaltung von Systemkomponenten, Systemen und Verarbeitungsketten, die einen Austausch von Komponenten bzw. Systemen in angemessener Zeit und zu vertretbaren Kosten ermöglicht. Je nach Relevanz kann es erforderlich sein, alternative Systemkomponenten oder Systeme explizit zu beauftragen, wenn diese ansonsten nicht in der erforderlichen Qualität, mit dem erforderlichen Funktionsumfang oder entsprechend den Sicherheitsanforderungen der Organisation verfügbar sind. Dies setzt insbesondere informationstechnische Grundkenntnisse in Bezug auf LLMs und LLM-Systeme voraus.

Auf der Ebene der Bereitsteller, etwa der IT-Dienstleister der öffentlichen Verwaltung, müssen erforderliche Kenntnisse und Ressourcen zum Aufgreifen von Forschungs- und Entwicklungsthemen und zum Umsetzen und Anpassen von Produkten (Forschungs-, Entwicklungs-, Produkt- und Betriebssouveränität) vorhanden sein. Gerade weil es im Bereich LLM-basierter KI-Lösungen derzeit noch eher selten um komplette Eigenentwicklungen geht, muss es den Bereitstellern möglich sein, sich qualifiziert mit den Herstellern am Markt rückzukoppeln, um Lösungen angemessen mitzugestalten. Das strategische Ziel ist hier: *Gestaltungsfähigkeit*. Dies setzt primär bei den organisationsinternen digitalisierungsbezogenen Kompetenzen an. Einen Großteil dieser digitalisierungsbezogenen Kompetenzen – bestehend aus Mindset (Grundeinstellung zur Digitalisierung), Kenntnissen und Fähigkeiten – und der digitaltechnischen Möglichkeiten hat die betrachtete Organisation selbst in der Hand, ausreichende finanzielle und personelle Mittel vorausgesetzt. Das Ziel *Gestaltungsfähigkeit* fokussiert somit darauf, Systeme (technisch) zu verstehen und umfänglich bewerten sowie deren Betrieb und Weiterentwicklung sicherstellen zu können. Die Bewertung muss funktional, technisch, unter Sicherheits-, wirtschaftlichen, (organisations-)politischen und strategischen Gesichtspunkten erfolgen.

Abbildung 1: Bedeutung Digitaler Souveränität, vgl. (IT-Planungsrat 2021)

Auf der Ebene der Auftraggeber – Beschaffungsstellen, aber auch beauftragende IT-Dienstleister – müssen Informationen und Wissen über Technologien zugänglich sein und Kompetenzen zu Bewertung von Ressourcen, Systemen, Komponenten und Sachverhalten (Wissens- und Transparenzsouveränität) vorgehalten werden. Die Auftraggeber sollten auf mehrere wettbewerbsfähige Anbieter zurückgreifen und durch das Setzen von realistischen Vorgaben einen Einfluss auf die Gestaltung des Angebotes am Markt nehmen können. Ferner müssen verbindliche Rahmenbedingungen zu Informationssicherheit und Datenschutz durchsetzbar sein. Das strategische Ziel lautet: *Einfluss auf Anbieter.* Dieses Ziel markiert in einem Auftraggeber-Auftragnehmer-Verhältnis den dynamischen Grenzbereich der Machtverteilung zwischen den beteiligten Parteien. Insbesondere, wenn es gelingt, Auftraggeber mit ähnlichen Souveränitätsanforderungen zusammenzubringen und gemeinsam gegenüber dem Auftragnehmer auftreten zu lassen, besteht oft die Chance, die Einflussmöglichkeit der Auftraggeber zu erhöhen, ohne dass diese durch die Zusammenarbeit der Auftraggeber wiederum Abstriche an ihrer faktischen Selbstbestimmung machen müssen.

Orthogonal zu den beschriebenen drei strategischen Zielen und den aus ihnen (über den Zwischenschritt der Lösungsansätze) abgeleiteten Maßnahmen steht das Technologie-Bündel (Mohabbat Kar und Thapa 2020, 12 f.) als ein Instrument zur Einordnung von Abhängigkeiten (Ist-Analyse; bottom-up) sowie zur Konkretisierung und zur Evaluation von Maßnahmen zur Steigerung der digitalen Souveränität (Soll-Analyse; top-down) zur Verfügung. Das Technologie-Bündel ist ein Modell, das digitale Systeme als Komposition aus bis zu fünf informationstechnischen Komponentenclustern betrachtet: Software-, Netze-, Hardware-, Daten-, und Plattformcluster.

Ein digitales System auf der Komponentenebene zu betrachten, um dessen digitale Souveränität zu bewerten, ist allerdings nur sinnvoll, wenn dies andere Perspektiven als eine rein monolithische Betrachtung des Systems ermöglicht. Die Nützlichkeit dieser Herangehensweise zeigt sich jedoch bei manchen Lösungsansätzen oder Maßnahmen deutlich: Herstellerunabhängige Modularität, (offene) Standards und Schnittstellen beispielsweise adressieren explizit Anforderungen, die sich auf Komponentenebene wiederfinden. Ein Wechsel von Softwaremodulen beispielsweise sollte ohne Anpassung der Hardware oder der Daten(-strukturen), aber auch ohne Einfluss auf gleichzeitig eingesetzte Softwaremodule möglich sein. In dem Kontext LLM-basierter KI-Lösungen müssen aus dem Technologie-Bündel also diejenigen Komponentencluster betrachtet werden, für die spezifische, vom »normalen Maß« abweichende Anforderungen gelten. Zentral ist dabei der Softwarecluster: Dort ist das LLM (bzw. sind die gemeinsam oder alternativ eingesetzten LLMs) angesiedelt, aber auch andere Softwarekomponenten, in die die LLMs eingebettet sind (für einen Überblick der Komponenten eines LLM-Systems siehe auch Abschnitt 1.2).

Spezifisch für LLM-basierte KI-Lösungen sind ebenfalls Hardwareanforderungen, weil der Betrieb, aber besonders das Training von LLMs bisher auf massive GPU-Rechenkapazitäten angewiesen sind, deren Verfügbarkeit eine zentrale Herausforderung darstellt (Horstmann 2024). Durch diese Anforderungen können unmittelbare Abhängigkeiten bestehen, die dem Hardwarecluster zuzuordnen sind, wenn die Hardware selbst beschafft und betrieben werden soll: Beispiele sind mangelnde Anbietervielfalt oder politisch bedingte Lieferunsicherheiten. Wenn hingegen beispielsweise Hardwareressourcen, die LLM-Nutzung oder die Nutzung kompletter LLM-basierter KI-Lösungen von Drittanbietern (z. B. Public-Cloud-Anbieter) gemietet werden, können unerwünschte Abhängigkeiten von diesen Dienstleistern entstehen, die dem Plattformencluster zuzurechnen sind. Auch der Datencluster kann betroffen sein, sofern nicht-öffentliche Daten in fremden Rechenzentren und teilweise außerhalb Deutschlands und der EU verarbeitet werden.

Unabhängig von der architekturellen und geografischen Verteilung der Komponenten einer LLM-basierten KI-Lösung sind spezifische Anforderungen an den Netzecluster nur in Spezialfällen zu beobachten. Netzbezogene Datenschutzanforderungen müssen zwar erfüllt sein, dies kann aber mit denselben

Lösungen erfolgen, die auch bei anderen verteilten IT-Systemen zum Einsatz kommen. Das heißt, dass KI-Systeme im Normalfall keine neuen spezifischen Souveränitätsanforderungen bezogen auf das Netzecluster einführen.

Zusammenfassend lässt sich also sagen, dass Abhängigkeiten vor allem im Softwarecluster und im Hardwarecluster, je nach Ausgestaltung der Lösung aber auch im Plattformcluster oder im Datencluster entstehen können.

1.2 Künstliche Intelligenz und große Sprachmodelle

Künstliche Intelligenz (KI) ist ein Ober- und Sammelbegriff für unterschiedliche Ansätze und Methoden mit denen versucht wird, Maschinen »intelligentes« Verhalten zu ermöglichen. Der europäische AI-Act definiert KI als

»ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können« (Verordnung (EU) 2024/1689).

Das maschinelle Lernen ist eine Unterklasse von KI (siehe auch Abbildung 2) und umfasst statistische Methoden, welche auf Basis von Daten funktionieren. Es handelt sich um Algorithmen, die »lernen«, also gegebene Informationen generalisieren und Regeln ableiten, um so Aussagen über neue Daten treffen zu können. Als die in den letzten Jahren erfolgreichste Methode haben sich »Neuronale Netze« durchgesetzt. Die ursprünglich lose von biologischen neuronalen Netzwerken inspirierten Modelle bestehen aus einem verknüpften Netz von Knoten, sogenannten Neuronen, die meist in Schichten organisiert sind. Das schrittweise, gezielte Anpassen der Gewichtung der Kanten wird als Training bezeichnet. Über die Gewichtung der Kanten (auch Gewichte genannt) in Verbindung mit der Eingabe wird die Ausgabe des neuronalen Netzes berechnet.

Durch die Vergrößerung des Netzes durch Hinzufügen weiterer Schichten und damit Knoten und Kanten kann das Modell mehr Information speichern. Solche »tiefen« Netze zu erzeugen, bezeichnet man als Deep Learning. Viele Fortschritte und Durchbrüche von KI sind neben architektonischen Anpassungen der Modelle vor allem auch der Vergrößerung der Netze zu verdanken, also dem Hinzufügen von mehr trainierbaren Parametern.

Generative KI (GenKI) zeichnet aus, dass sie auf Basis der zugrunde liegenden Daten eigenständig neue Daten generieren kann, beispielsweise Text, Bilder oder Videos. Alle modernen

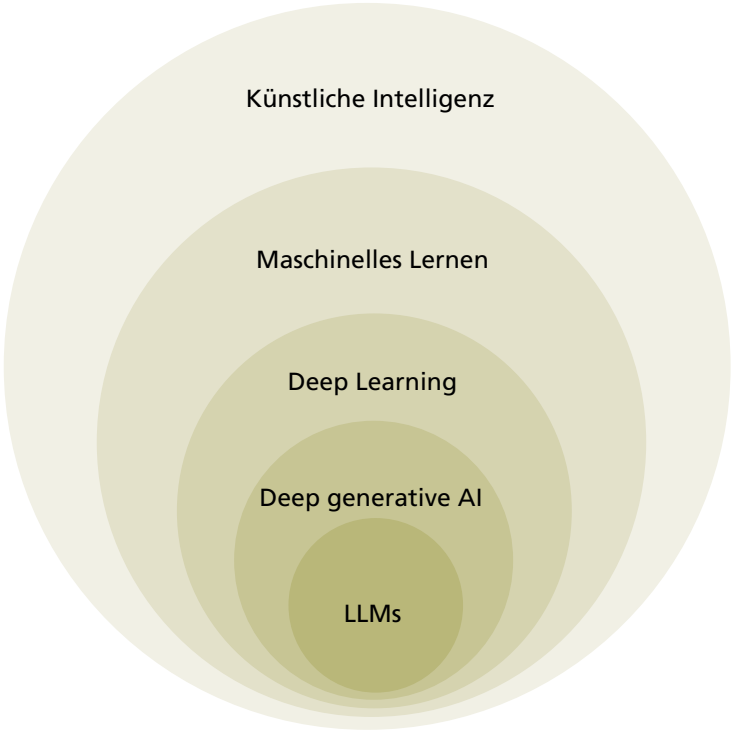


Abbildung 2: Begriffliche Verortung von LLMs, eigene Darstellung

Jahr der Veröffentlichung	LLMs	Anzahl Parameter	Entwickler
2017	Transformer	530 Millionen	Google AI
2018	BERT	340 Millionen	Google AI
2019	GPT-2	1.5 Milliarden	OpenAI
2020	GPT-3	175 Milliarden	OpenAI
2022	LaMDA	127 Milliarden	Google AI
2022	GPT-3.5	175 Milliarden	OpenAI
2023	LLaMA	65 Milliarden	Meta AI
2023	GPT-4	1-1.76 Billionen	OpenAI
2023	Gemini	Nicht angegeben	Google AI
2023	Mistral 7B	7 Milliarden	Mistral
2024	LLaMA 3	8 & 70 Milliarden	Meta AI
2024	Luminous	~13 Milliarden	Aleph Alpha
2025	DeepSeek-V3	~ 670 Milliarden	DeepSeek

Tabelle 1: Die Parameteranzahl der größten LLMs und die zugehörigen Entwickler (vgl. unter anderem Hagos et al. 2024)

GenKI-Modelle lassen sich dem Deep Learning zuordnen. Wenn diese Systeme nicht für einen konkreten Einsatzzweck entwickelt, sondern so trainiert wurden, dass sie eine Vielzahl unterschiedlicher Aufgaben bearbeiten können, werden sie in der KI-Verordnung als »ein KI-Modell mit allgemeinem Verwendungszweck« gefasst. Das ist

»ein KI-Modell – einschließlich der Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird –, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden« (Verordnung (EU) 2024/1689).

Mathematisch gesehen ist ein generatives Modell eine Funktion, welche die einer Datenmenge zugrunde liegende Wahrscheinlichkeitsverteilung approximiert. Wenn die modellierte Verteilung der Ursprungsverteilung ausreichend ähnelt, ähneln auch die generierten Daten den Originaldaten. Hier haben sich in den letzten Jahren vor allem autoregressive Modelle durchgesetzt. Solche Modelle verarbeiten sequenzielle Daten und machen auf dieser Basis Vorhersagen.

Da Sprache und Text sequenzieller Natur sind, eignen eignet sich dieser Modelltyp dafür sehr gut. Diese Studie fokussiert auf solche Modelle, sogenannte Sprachmodelle. Die rasanten Entwicklungen der jüngsten Zeit wurden durch eine Kombination mehrerer Faktoren ermöglicht, die sich gegenseitig bedingen. Dazu zählen vor allem:

- Höhere bzw. mehr parallele Rechenleistung (schnellere GPUs)
- Zugang zu und Nutzbarmachung von mehr Daten
- Bessere Algorithmen, vor allem im Bereich Deep Learning
- Transfer-Learning und Pre-Training
- Moderne Architekturen wie Transformer und Autoencoder
- Kollaborationsplattformen und hohe Open-Source-Anteile bei KI-Entwicklung

Die Durchbrüche der letzten Jahre bei Sprachmodellen sind auch auf die Erhöhung der Anzahl der trainierbaren Parameter zurückzuführen, veranschaulicht in Tabelle 1 (was wiederum nur möglich wurde, weil die Hardware entsprechend leistungsfähiger wurde und immer größere Datenmengen zur Verfügung stehen). Zur Veranschaulichung: Ein bekannter Benchmark ist Massive Multitask Language Understanding (MMLU), bei dem das Wissen und Verständnis eines Modells über viele verschiedene Themen evaluiert wird. Ein frühes Modell wie GPT-2 (2019) besitzt eine Parameteranzahl von etwa 1,5 Milliarden und liegt bei MMLU im Durchschnitt bei 32,4 Prozent. Bei dem jüngeren Modell GPT-4 (2023) ist die Parameteranzahl auf eine Billion gestiegen, der Score liegt bei 87 Prozent (Papers With Code 2025). Ab einer Zahl von einer Milliarde Parametern wird meist von »großen« Sprachmodellen gesprochen. Es sind diese großen Modelle, die in den letzten Jahren die meiste Aufmerksamkeit erzeugt haben.

Ein vereinfachtes Ablaufschema der Entwicklung einer LLM-Anwendung bis hin zur Nutzung ist in Abbildung 3 zu sehen. Ausgehend von einer geeigneten Architektur wird das »leere«

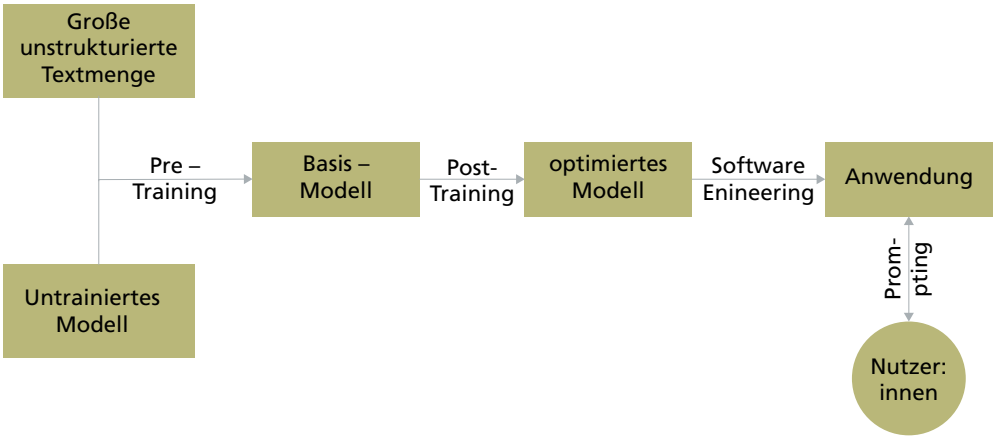


Abbildung 3: LLM vereinfachtes Ablaufschema vom Modell zur Nutzung

Modell im ersten Schritt, dem sogenannten »Pre-Training«, mit enormen Mengen Daten – typischerweise aus dem Internet – in nicht-überwachtem Stil »unsupervised« trainiert. Das Pre-Training großer Sprachmodelle ist mit offenen Urheberrechtsfragen und mit hohen Kosten verbunden und benötigt spezielle Hardwareressourcen mit viel Rechenkapazitäten, die einen hohen Stromverbrauch verursachen. Das so trainierte Basis-Modell verfügt über die Fähigkeit, kohärente grammatische Satzstrukturen zu bilden und kann auf das gewissermaßen »eingebettete« Wissen aus den Trainingsdaten zurückgreifen. Das Modell »weiß« z. B. nun mit hoher Wahrscheinlichkeit, dass ein Frosch eher grün als blau oder rot ist.

Nach dem Pre-Training folgt ein zweiter Trainingsschritt, um das Basis-Modell zu optimieren, sogenanntes Post-Training (oder auch Feintuning). Dieses ist, anders als im Schritt zuvor, zumeist überwachtes Lernen oder verstärkendes Lernen. Für diesen Schritt braucht es sorgfältig aufbereitete, hochwertige Daten, die von Menschen kuratiert, also mindestens verschlagwortet und gefiltert wurden. Dieser Schritt kann sehr arbeitsintensiv sein, wenn nicht auf bestehendes Material zurückgegriffen wird, wo der Aufwand damit jedoch lediglich »outgesourced« wurde. Somit zahlt dieser Trainingsschritt darauf ein, dem Modell das »gewünschte« Verhalten beizubringen. Was unter »gewünscht« zu verstehen ist, ist dabei jedoch keineswegs eindeutig. Werte, ethische Grundhaltungen und Normen prägen das gesellschaftliche Verständnis wünschenswerten Verhaltens, doch diese variieren je nach kulturellem Hintergrund. Aus Souveränitätsperspektive bietet die Optimierung durch Post-Training somit die Möglichkeit, den Output der Modelle nach eigenen Wertevorstellungen wie auch sozialen und rechtlichen Normen zu gestalten. Auf diesem Weg wird versucht sicherzustellen, dass die Systeme ethische Grundsätze wie Fairness und Inklusion, Schadenvermeidung und Gemeinwohl berücksichtigen.

Das auf diese Weise optimierte Modell kann als eine Komponente in eine Anwendung integriert werden. Zu einer solchen Anwendung gehören neben einem Frontend (zum Beispiel in Form eines Web-Interface oder auch Office-Plugin) ein Backend mit Datenverarbeitungsinfrastruktur und gegebenenfalls Möglichkeiten zum Filtern unerwünschter Ergebnisse. Außerdem können Methoden des Prompt Engineering zum Einsatz kommen, um dem Modell ein gewünschtes Verhalten beizubringen. Die rechenintensiven Prozesse der Antwortgenerierung (Inferenz) werden häufig auf Server mit entsprechender Hardware ausgelagert. Dabei kann es sich um »hausinterne« Hardware, von öffentlichen Einrichtungen gemeinsam genutzte Server oder um Angebote kommerzieller, privater Cloudanbieter handeln.

Es gibt derzeit einen Ansatz, LLMs durch Software zu ergänzen, um Probleme zu lösen, für die LLMs nicht optimiert sind. Diese Systeme werden auch als **KI-Agenten** bezeichnet.

KI-Agenten werden von einem optimierten Modell (siehe auch Abbildung 3) ausgehend für ein bestimmtes Aufgabenprofil (wie beispielsweise Recherche oder Kundendienst) konzipiert. Zum Wesenskern von KI-Agenten gehört die weitestgehend eigenständige Bearbeitung einer Aufgabe unter Berücksichtigung der bereitgestellten digitalen Werkzeuge (z. B. Taschenrechner, Kalender, Internetsuche) und des gegebenen Kontexts. Das bedeutet, dass dem LLM Zugang zu Softwarewerkzeugen gegeben und eine »Wahrnehmung« der relevanten, zumeist virtuellen Umgebung (z. B. Internetseiten, Software, Mailaccounts) ermöglicht wird.

KI-Agenten bestehen typischerweise aus vier wesentlichen Komponenten (siehe Abbildung 4). Das LLM funktioniert hier als das Entscheidungszentrum, das diese Komponenten steuert und damit das Gesamtsystem in die Lage versetzt, (autonom) größere Aufgabenkomplexe zu bearbeiten, also Aktionen auszuführen. Eine Aktion, oder auch Handlung eines KI-Agenten, kann von einer simplen Textausgabe bis hin zum Auslösen von Ereignissen in der physischen Welt reichen. Das Entscheidungszentrum nutzt Methoden der Planung, unter anderem die Zerlegung größerer Aufgaben in kleinteiligere Zwischenziele. Weiterhin hat es typischerweise Zugriff auf verschiedene digitale Werkzeuge, an welche spezifische Aufgaben ausgelagert werden können. Je nach Aufgabenfeld, in dem sich der KI-Agent befindet, können auch unterschiedliche Kontextinformationen einfließen. Das Gedächtnis eines KI-Agenten ist verantwortlich für die Speicherung von Informationen und Wissen. Darüber hinaus sind einige KI-Agenten in der Lage, im Laufe ihres gesamten Einsatzes kontinuierlich zu lernen.

KI-Agenten sind also komplexe Software-Systeme, die selbstständig in ihrer (virtuellen) Umgebung agieren, um unterschiedliche Ziele zu erreichen. Sie sind schon lange Gegenstand der Forschung. Das aktuelle Interesse an KI-Agenten ist maßgeblich auf den Erfolg von LLMs als zentraler Komponente zurückzuführen, denn diese besitzen Eigenschaften, die sich für die Anforderungen eines Entscheidungszentrums besonders gut eignen. Auch wenn aktuell nicht davon auszugehen ist, dass KI-Agenten demnächst Arbeitspakete innerhalb von Verwaltungen selbstständig bearbeiten werden, sollte der Trend weiterhin beobachtet werden. Es ist davon auszugehen, dass LLMs in ihren Fähigkeiten »Planung« und »Gedächtnis« weiter besser werden, und die Integration von Werkzeugen zur Bewältigung der (Teil-)Aufgaben, für die LLMs nicht ausgelegt sind, erhöht den Funktionsumfang und die Effizienz der Aufgabenerledigung beträchtlich.

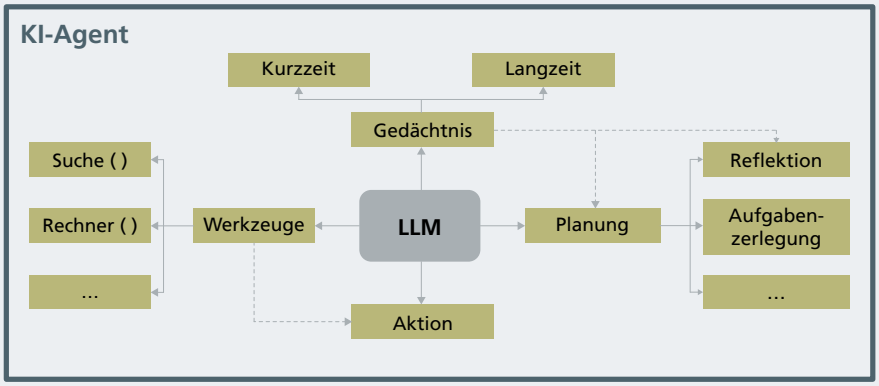


Abbildung 4: Übersicht eines LLM-basierten autonomen Agenten (vgl. Weng 2023)

2. Analysemethodik

Nach der Einführung der wesentlichen Konzepte soll nun das Vorgehen zur Untersuchung der auf der Ebene der Bundesverwaltung in Entwicklung oder in Betrieb befindlichen LLM-Systeme beschrieben werden. Die zu beantwortende Frage lautet:

Wie ist die Bundesverwaltung in ihren Rollen als Bereitsteller, Entwickler und Auftraggeber bezogen auf Anwendungen großer Sprachmodelle bei der Erfüllung der strategischen Souveränitätsziele Wechselmöglichkeit, Gestaltungsfähigkeit und Einfluss auf die Anbieter aufgestellt?

Im Fokus der Untersuchung steht die Identifikation von bestehenden oder neu entstehenden Abhängigkeiten bei Eigenentwicklungen oder Beauftragungen von Systemen mit großen Sprachmodellen (LLMs). Abhängigkeiten können durch eine Vielzahl von Faktoren entstehen, unter anderem durch die Beschaffenheit der IT-Landschaft, von Prozessen, Personal, Verträgen oder Marktgegebenheiten. Der damit einhergehende Kontrollverlust kann zu sogenannten Schmerzpunkten führen. Zu möglichen Schmerzpunkten zählen beispielsweise eingeschränkte Informationssicherheit, rechtliche Unsicherheiten, unkontrollierbare Kosten, eingeschränkte Flexibilität oder fremdgesteuerte Innovationen (PwC 2019).

Als Datengrundlage für diese Studie dient der vom BMI bereitgestellte, online zugängliche »Marktplatz der KI-Möglichkeiten« (MaKI), der zum Stichtag 01.02.2025 insgesamt 182 Projekte listete und damit »einen umfassenden Überblick über den Einsatz von KI in der Bundesverwaltung« (Bundesministerium des Innern (BMI) 2025) bietet. Zur Beantwortung der oben genannten Forschungsfrage wurde ein Vorgehen entwickelt, welches die nachfolgenden sechs Schritten umfasst:

1. **KI-Marktbetrachtung:** Metaanalyse von 14 internationalen LLM-Marktstudien zu den größten Anbietern
2. **Maßnahmenanalyse:** Bestandaufnahme von laufenden Maßnahmen, die digitale Souveränität im Kontext LLM-basierter KI-Lösungen in Deutschland fördern; Analyse zum Umgang mit digitaler Souveränität im Ausland
3. **Indikatorerstellung:** Literaturrecherche und Experteninterviews zur Identifikation von Indikatoren für die drei strategischen Souveränitätsziele und ihre Zusammenführung in einer Analysematrix
4. **Datenerhebung:** Identifikation relevanter (LLM-basierter) Projekte im MaKI mit anschließender Datenerfassung mittels eines Online-Erhebungsbogens
5. **Identifikation Schmerzpunkte:** Erstellung eines Index zur Abschätzung möglicher Schmerzpunkte bei Entwicklung und Betrieb von LLMs mithilfe der Zusammenführung von Indikatoren und Daten in der Analysematrix
6. **Vertiefende Projektinterviews:** Interviews mit Verantwortlichen aus fünf Projekten zu spezifischen Projektaspekten, Schmerzpunkten und Handlungsempfehlungen

Im ersten Schritt sollte ein Überblick über die aktuelle Marktlage gewonnen werden. Dies erschien wichtig, da es sich um einen jungen, aber sehr dynamischen Markt handelt, der zwar von einigen der großen Technologieunternehmen geprägt, aber noch nicht vollständig dominiert scheint. Außerdem sollte ein Blick auf die Marktverfügbarkeit von spezifisch für den öffentlichen Sektor optimierten Lösungen geworfen werden. Zwei der Ziele digitaler Souveränität (*Wechselmöglichkeit*, *Einfluss auf Anbieter*) stehen damit in Verbindung.

Im zweiten Schritt wurden die bestehenden Maßnahmen für digitale Souveränität in dem spezifischen Kontext KI und konkreter LLMs untersucht. Parallel dazu wurden auch der Blick ins Ausland geworfen und aus insgesamt 22 Ländern Digitalstrategien im Hinblick auf digitale Souveränität analysiert. Damit sollte sich dem Thema aus strategischen Gesichtspunkten genähert werden, welche als Überbau für die anschließende Untersuchung dienten.

Für eine Einschätzung der digitalen Souveränitätsziele bei den Eigenentwicklungen der Bundesverwaltung wurden geeignete Indikatoren benötigt. Dazu wurden in Schritt (3) einschlägige Literatur gesichtet und Interviews mit Expert:innen des Fraunhofer-Instituts für offene Kommunikationssysteme (FOKUS) geführt. Die Indiktorenentwicklung orientierte sich an einem

Vorschlag zur Weiterentwicklung der Wirtschaftlichkeitsbetrachtung (WiBe) für IT-Beschaffungen um Souveränitätsaspekte. Dabei wurden die Ausprägungsstufen zugunsten einer einfacheren Erhebbarkeit stark reduziert und beispielsweise auf maximal vier Ausprägungen begrenzt. Jeder Indikator zahlt auf eines oder mehrere der Souveränitätsziele *Wechselmöglichkeit*, *Gestaltungsfähigkeit* und *Einfluss auf Anbieter* ein.

Die Indikatoren bilden auch die Grundlage für den Erhebungsbogen im vierten Schritt. Zur Entwicklung des Erhebungsbogens wurden die Indikatoren mit den auf dem »Marktplatz der KI-Möglichkeiten« (MaKI) verfügbaren Daten verglichen, um die noch zu erhebenden Daten zu bestimmen. Die Entwicklung des Erhebungsinstruments erfolgte dabei unter der Prämisse, den Aufwand für die Projektverantwortlichen möglichst gering zu halten – nicht zuletzt auch, um die Antwortbereitschaft zu erhöhen. Daher wurde auf eine tiefgehende technische Betrachtung verzichtet, sondern vielmehr mit den Fragen eine »angemessene Flughöhe« angestrebt.

Auf Basis aller verfügbaren Daten wurde im fünften Schritt die Analyse durchgeführt. Dafür wurde ein »Ist-Soll-Zustand«-Ansatz verfolgt. Es wurde ein projektunabhängiger Soll-Zustand durch die möglichen Ausprägungen der Indikatoren definiert, anhand dessen alle Projekte risikounabhängig bewertet werden (siehe dazu Anhang A.5). Die maximalen Werte der Indikatoren definieren somit den Soll-Zustand. Die Ausprägungen der einzelnen Projekte wurden in der Indikatormatrix aggregiert und somit Scores für die drei strategischen Ziele berechnet. Diese dienten als Basis, um mögliche Schmerzpunkte in Bezug auf digitale Souveränität zu identifizieren. Im Rahmen dieser Studie wurde ein solcher projektunabhängiger Ansatz gewählt, da es aufgrund der Menge der Projekte unrealistisch erschien, für jedes einzelne eine Risikoanalyse durchzuführen.

In Schritt (6) wurden mit einer Reihe von Projekten vertiefende Interviews mit jeweils unterschiedlichem Schwerpunkt geführt. Dabei wurden unter anderem sich abzeichnende Schmerzpunkte thematisiert und offene technische und organisationale Fragen geklärt. Ebenfalls wurde nach konkreten Vorschlägen gefragt, wie digitale Souveränität aus Sicht der Projekte gestärkt werden könnte.

3. Anbieter und Angebote

3.1 Marktbetrachtung Sprachmodelle

Marktgröße

Für die Analyse des Marktes für große Sprachmodelle wurde eine Metaanalyse von 14 internationalen LLM-Marktstudien durchgeführt, die zwischen 2023 und 2025 veröffentlicht wurden (die Liste der Marktstudien findet sich im Anhang A.2). Der globale Markt für große Sprachmodelle betrug 2023 je nach Bemessungsgrundlage zwischen 1,6 und 4,5 Mrd. US-Dollar mit einer erwarteten kumulierten jährlichen Wachstumsrate von 23,5 bis zu 79,8 Prozent. Die großen Spannbreiten demonstrieren die hohe Dynamik des Marktes, die eine Bewertung und verlässliche Vorhersage erschweren. Der größte Markt war 2023 Nordamerika mit etwa 35 Prozent des weltweiten Umsatzes, gefolgt vom asiatisch-pazifischen Raum mit 30 Prozent und Europa mit 20 bis 25 Prozent (je nach Schätzung), wobei dem asiatisch-pazifischen Raum die höchsten Wachstumsraten vorhergesagt wurden.

Marktstruktur

Betrachtet man die Marktstruktur, so zeigt sich eine klare Dominanz der führenden Anbieter, die 2023 88,2 Prozent des Gesamtumsatzes erzielten (Intel Market Research 2024). In den analysierten Publikationen wurden als Marktführer OpenAI, Google und Meta genannt. Der Markt kann damit als relativ konzentriert angesehen werden, zugleich zeigt sich aber eine intensive Konkurrenz der Marktführer untereinander, zu erkennen an hohen Investitionen in Forschung und Entwicklung sowie immer neuen Allianzen und Übernahmen. Während die hohe Dynamik und Innovationskraft weiterhin viele neue Wettbewerbende insbesondere für Nischenmärkte hervorbringt, gibt es ebenfalls Treiber, die eine Konzentration des Marktes begünstigen, unter anderem durch ungleichen Zugang zu Daten, Rechenleistung und Kapital (Thun und Hanley 2024). Dass auch die globale Marktstruktur noch nicht sehr gefestigt ist und erfolgreiche Markteintritte bei allgemeinen Sprachmodellen möglich sind, zeigen unter anderem die Marktverschiebungen durch den Release des chinesischen DeepSeek-Modells R1 im Januar 2025.

Marktführer

Neben OpenAI, Google und Meta als Marktführer wurden besonders häufig die nachfolgenden genannt: Microsoft (Turing-NLG, Orca) (USA), Tencent (Hunyuan) (China), Baidu (Ernie) (China), Alibaba (Qwen) (China), Huawei (Pangu) (China), AI21 Labs (Jurassic) (Israel) und Yandex (YaLM) (Russland).

Von den 10 Unternehmen stammen je vier aus den USA und aus China. Europäische oder gar deutsche Unternehmen spielen auf dem Weltmarkt eine untergeordnete Rolle, einzelne Unternehmen, die im Kontext von LLMs in den Marktanalysen untersucht werden, sind unter anderem SAP (Deutschland), Mistral (Frankreich), Neuralfinity (Deutschland), Stability AI (UK) oder LightOn (Frankreich). Wenig überraschend dominiert Nordamerika damit den Markt, mit einem geschätzten Marktanteil von 33 bis zu 53 Prozent des weltweiten Umsatzes im Jahr 2023. So kommt Microsoft auf einen signifikanten Anteil von geschätzten 39 Prozent im KI-Segment für Basis-Modelle (LLMs sind als eine spezifische Form von Basis-Modellen auf die Verarbeitung von Sprache ausgerichtet) und Plattformen, gefolgt von AWS mit 19 Prozent und Google mit 15 Prozent (Fernandez 2025). Der asiatisch-pazifische Raum kam 2023 auf 22 bis 26 Prozent des weltweiten Umsatzes, Europa immerhin noch auf 17 bis 31 Prozent. Zahlen vom Mai 2024 zeigen, dass fast 67 Prozent der Organisationen weltweit LLM-gestützte Produkte nutzen (Uspenskyi 2025). Die wichtigsten Branchen sind hierbei Einzelhandel und E-Commerce, Finanzen und Versicherungen, Gesundheit, Bildung sowie Medien und Unterhaltung. Staatliche Anwendungen haben eine geringe Relevanz. Die Performanz der Modelle ist jedoch nicht für alle Aufgaben und Branchen und in allen Sprachen gleich hoch, weswegen die Marktstrukturen regional und je nach Aufgabe und Endkundensegment variieren. Neben den globalen gibt es deshalb auch eine Vielzahl regionaler und spezialisierter Anbieter, sodass sich der Markt regional und nach Branche und Aufgabe fragmentierter darstellt, als dies ein Blick auf die weltweiten Branchenführer vermuten lässt. Zudem ermöglicht die unterschiedlich gute Performanz bei Aufgabe und Sprache den Markteintritt für spezialisierte Anbieter und Modelle in Nischenmärkten, wie beispielsweise Teuken. Bei Teuken handelt es sich um ein multilinguales Open-Source-Modell, das für einige europäische

Sprachen eine deutlich höhere Leistungsfähigkeit aufweisen soll als vergleichbare Modelle. Auch Aleph Alpha, ein deutsches KI-Unternehmen, hat mit PhariaAI eine neue KI-Architektur vorgestellt, welche effizienter an neue Sprachen oder spezialisiertes Fachwissen angepasst werden kann.

Abhängigkeiten mit oder zu anderen Märkten

Große Sprachmodelle benötigen hoch performante Chips. Hier hat Nvidia (USA) annähernd ein Monopol, mit einem Marktanteil von 92 Prozent bei Datencenter-GPUs (Korinek und Vipra 2024; Fernandez 2025) und etwa 80 Prozent für KI-Chips (Holzki 2025) samt ihres korrespondierenden Ökosystems, das etwa die Softwareplattform CUDA umfasst. Obwohl es seitens der großen Sprachmodell-Anbieter derzeit Bestrebungen gibt, sich etwas aus dieser Abhängigkeit zu befreien (s. u. nachfolgender Abschnitt »Trends«), kann es sinnvoll sein, neben der Frage nach der digitalen Souveränität gegenüber den Anbietern großer Sprachmodelle auch die der digitalen Souveränität im Chip- bzw. generell im Hardwaremarkt genauer unter die Lupe zu nehmen. Getrieben durch den hohen Rechenbedarf von LLMs verzeichnet auch der entsprechende Hardwaremarkt gerade ein hohes Wachstum. Ähnliches gilt für den Cloudmarkt, in dem – je nach gewählter Bereitstellungsart und nicht nur im Kontext der Nutzung von LLMs – neue Abhängigkeiten entstehen können. Hier ist AWS zu nennen, das schon 2017 von Gartner als führender internationaler Anbieter von Cloud Computing eingestuft wurde (Gartner 2017). Die Muttergesellschaft von AWS, Amazon, ist unter anderem mit Titan und Olympus ebenfalls auf dem Markt für LLMs aktiv.

Trends

Der Markt für große Sprachmodelle ist von einer hohen Dynamik und Innovation geprägt. Große Unternehmen investieren weiterhin hohe Summen in Forschung und Entwicklung. So verkündete kürzlich Microsoft, bis Ende Juni 2025 weitere 80 Mrd. US-Dollar insbesondere in Rechenzentren zu investieren. Im Rahmen der US-amerikanischen «Stargate«-Initiative sollen 500 Mrd. US-Dollar in die physische und digitale Infrastruktur – vor allem in Rechenzentren – für das Training neuer KI-Modelle in den USA investiert werden. Der große Energiebedarf der KI-Modelle beeinflusst jedoch nicht nur die Ausstattung und Anbindung von Rechenzentren, sondern auch den Strommarkt, wie sich an Investitionen verschiedener LLM-Marktführer in Atomenergie oder andere Energiequellen ablesen lässt. Neben Forschung und Entwicklung spielen auch neue strategische Allianzen eine Rolle im Kampf um höhere Marktanteile. Beispielsweise können Entwickler:innen, die GitHub Copilot von Microsoft nutzen, nun zwischen verschiedenen Modellen, bspw. auch von Google und Anthropic, wechseln; zuvor konnten nur OpenAI-Modelle genutzt werden (Deutsche Bank Research 2024a). Zudem werden die KI-Modelle von OpenAI künftig nicht mehr exklusiv auf Microsoft-Servern gehostet, auch wenn Microsoft seinen Einfluss bei OpenAI vorerst behält.

Auch auf dem Chipmarkt wird die alles beherrschende Marktmacht von Nvidia zunehmend herausgefordert. So arbeitet OpenAI unter anderem mit Broadcom, TSMC und AMD zusammen, um seine ersten eigenen KI-Chips herzustellen, von denen die ersten ab 2026 geliefert werden sollen. Auch Google, Amazon, Meta und Microsoft hatten bereits Maßnahmen ergriffen, ihre Abhängigkeit von Nvidia zu reduzieren (Deutsche Bank Research 2024a). Weitere prägende Trends sind die zunehmende Bedeutung von Middleware, also Software, die zwischen Anwendung und LLMs angesiedelt ist, bei der sich weitere Marktmöglichkeiten (und in der Folge mögliche Abhängigkeiten) auftun, ein stärkerer Fokus auf leichtgewichtigere und spezialisiertere Modelle sowie die wachsende Bedeutung von erklärbarer KI, Ethik und Datenschutzaspekten, auch getrieben durch die EU-Regulierung großer Sprachmodelle. Diese Entwicklungen begünstigen auch das Aufkommen von und die Nachfrage nach Sicherheitslösungen, um Risiken bei der Nutzung von LLMs zu mindern, sowie nach Open-Source-Lösungen. Unter anderem Teuken-7b von OpenGPT-X und das Unternehmen EleutherAI verfolgen diesen Ansatz. Auf der technischen Ebene gilt es, das Aufkommen von KI-Agenten, die vollständige Handlungsroutinen selbstständig durchführen können, im Blick zu behalten. Hier haben unter anderem Anthropic, Microsoft und Salesforce kürzlich neue Produkte vorgestellt (Deutsche Bank Research 2024b).

3.2 Open Source bei LLMs

Der Markt großer Sprachmodelle weist einen bemerkenswert hohen Anteil quelloffener Produkte auf (Naveed et al. 2023). Verschiedene Hersteller werben mit der Offenheit ihrer KI-Systeme, die die Attraktivität der Produkte steigern soll. Doch was bedeutet Open Source in Bezug auf generative KI?

Die ersten großen Sprachmodelle, welche zwischen 2018 und 2021 veröffentlicht wurden, waren offene Modelle, was eine wissenschaftliche Nachvollziehbarkeit gewährleistete. Frühe LLMs wurden zunächst über Konferenzbeiträge oder als Preprint der Fachöffentlichkeit präsentiert, Code und oder Modellparameter wurden auf gängigen Social-Coding-Plattformen wie GitHub sowie später auch auf KI-spezifischen Plattformen wie Hugging Face zur Verfügung gestellt. Im Unterschied zu konventioneller Softwareentwicklung, die sich über Jahrzehnte die Praktiken offener und kollaborativer Governance erarbeitet hat, sticht Künstliche Intelligenz als eine der ersten flächendeckenden disruptiven Technologien heraus, die fest auf eine elaborierte Open-Source-Infrastruktur zurückgreifen kann. Mit dem Erfolg kommerzieller LLM-Systeme ab 2022 stieg die Zahl proprietärer Modelle deutlich an. Seit 2023 zeigt sich ein Wandel

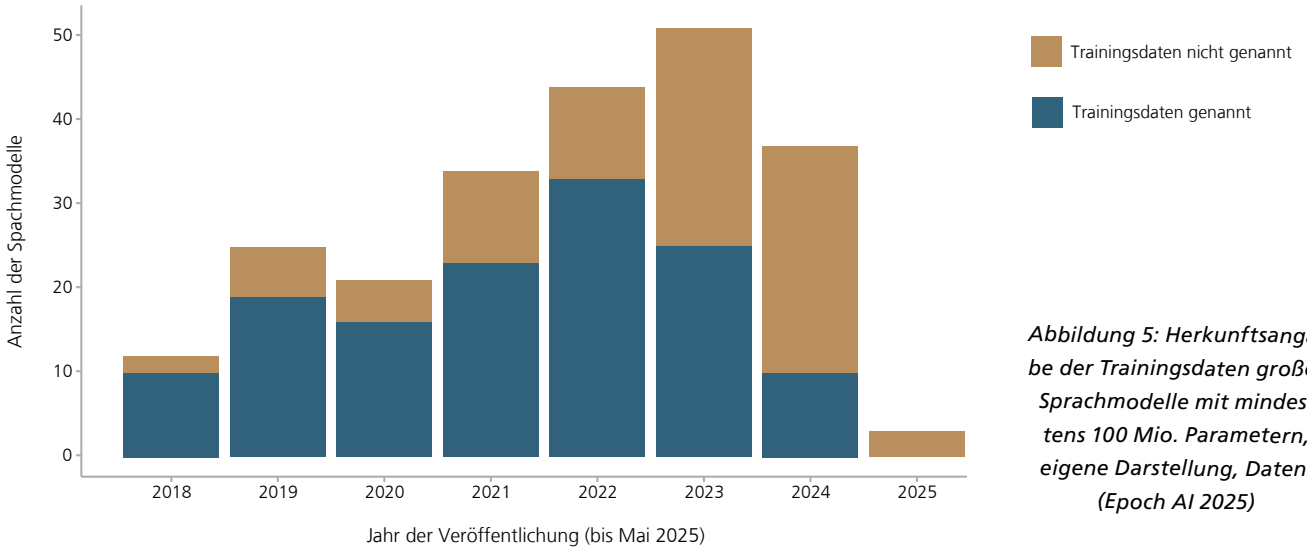


Abbildung 5: Herkunftsangabe der Trainingsdaten großer Sprachmodelle mit mindestens 100 Mio. Parametern, eigene Darstellung, Daten: (Epoch AI 2025)

im Offenheitsverständnis: Während echte Open-Source-Modelle seltener werden, konzentrieren sich Anbieter vermehrt auf die Öffnung einzelner Komponenten, etwa der Modellgewichte (»Open Weights«), Trainingsdaten und -code werden hingegen meist nicht veröffentlicht.

Konventionelle Open-Source-Software-Definitionen reichen nur eingeschränkt aus, um die Systeme und ihre zugrunde liegenden Sprachmodelle zu bewerten. War es bisher genug, Quellcode einer Software in Repositorien zu veröffentlichen, muss hier die Funktionsweise eines Sprachmodells auch in ihrer Entstehung, also in ihrem Training und im Feintuning, nachvollziehbar sein. Hierfür hat die Open Source Initiative im Herbst 2024 die erste Version der Open Source AI Definition herausgegeben (Open Source Initiative 2024), die durch Expert:innen kollaborativ erarbeitet wurde. Diese deckt sich größtenteils mit zuvor in wissenschaftlichen Erhebungen angewandten Messgrößen, siehe (Sowe et al. 2024) und (White et al. 2024). Auch die europäische Gesetzgebung berücksichtigt KI-Modelle, »die im Rahmen einer freien und quelloffenen Lizenz bereitgestellt werden«. So bleiben Open-Source-Modelle aufgrund ihrer Nachvollziehbarkeit von Pflichten und Vorgaben des AI Act weitestgehend unberührt.

Laut der Open Source Initiative gelten LLMs als vollumfänglich offen, wenn sie folgende Eigenschaften aufweisen:

- **Informationen zu Trainingsdaten liegen vor:** Damit eine rechtlich sichere Nutzung eines KI-Systems sichergestellt werden kann, sollten Angaben über den Bezugsort, die Auswahl, das Kennzeichnungsverfahren, Datenverarbeitungs- und Filtermethoden sowie den Anwendungsbereich unabdingbar sein. Offene Daten, die öffentlich abrufbar sind und eindeutig unter einer freien Lizenz stehen, sind bei der Wahl der Trainingsdaten vorzuziehen. Auffällig ist, dass seit 2023 die Beschreibung der Trainingsdaten immer seltener transparent gemacht wird, siehe auch Abbildung 5. Hersteller lassen die Herkunft der Daten häufig im Unklaren und der Verdacht besteht, dass hier Urheberrechtsverletzungen begangen werden.
- **Der Quellcode ist offen:** Die Offenlegung des Quellcodes für das Training und das Feintuning großer Sprachmodelle ist zentral für die Nachvollziehbarkeit und Reproduzierbarkeit. Während einige Organisationen zumindest Teile ihrer Trainingspipelines offenlegen, bleiben viele entscheidende Komponenten – insbesondere in der nachträglichen Optimierung – unveröffentlicht (Sowe et al. 2024).
- **Modell und Parameter sind offen:** Offene Modellgewichte sind für die Nachnutzung eines Sprachmodells zentral und die Mindestvoraussetzung, um von Open-Source-Modellen zu sprechen. Für eine höhere Nachvollziehbarkeit könnten idealerweise auch die Parameter relevanter Zwischenetappen beim Training des Modells offengelegt werden. Das bezieht sich auf den Trainingsprozess, der iterativ geschieht.
- **Standardisierte Evaluation ist erfolgt:** Ohne Transparenz bei Benchmarks, Testdaten und Bewertungskriterien ist ein objektiver Leistungsvergleich kaum möglich. Um eine Vergleichbarkeit zu ermöglichen, sollten standardisierte Evaluationsmethoden verwendet werden, um so die Qualität und Zuverlässigkeit von KI-Systemen nachvollziehbar zu machen. Die Veröffentlichung von Benchmarks findet vor allem über zitierfähige Preprints zum Zweck wissenschaftlicher Reputation statt.
- **Partizipation und Mitbestimmung ist gewährleistet:** Open Source bedeutet auch Zusammenarbeit und Mitbestimmung. In bisherigen Untersuchungen wurde hierfür zum Beispiel die Interaktion zwischen Entwickler:innen und Nutzer:innen innerhalb der Projektrepositorien ausgewertet. Hersteller sollten darüber hinaus auch möglichst offen projektstrategische Entscheidungen mit der Community teilen.

4. Maßnahmen zur digitalen Souveränität im Bereich KI

Ausgehend von verschiedenen Programmen, Strategien und Vereinbarungen, so unter anderem dem Koalitionsvertrag (»Verantwortung für Deutschland« (CDU et al. 2025)), der Datenstrategie der Bundesregierung (»Fortschritt durch Datennutzung« (ehemals Bundesministerium für Digitales und Verkehr (BMDV) 2023)), der »Strategie zur Stärkung der digitalen Souveränität für die IT der Öffentlichen Verwaltung« des IT-Planungsrates (IT-Planungsrat 2021) und dem Beschluss der Konferenz der Regierungschefinnen und Regierungschefs der Länder »Technologische Souveränität sichern – KI-Standorte Europa und Deutschland stärken« (MPK 2025) wurden in der Vergangenheit bereits eine Reihe von Forderungen staatlicher Akteure aufgestellt sowie Maßnahmen in die Wege geleitet, die der digitalen Souveränität Deutschlands im Hinblick auf Künstliche Intelligenz dienlich sein können.

4.1 Überblick laufende Maßnahmen

Die öffentliche Hand sieht sich selbst (Capgemini 2025) als eine wesentliche zukünftige Nutzerin LLM-basierter KI-Lösungen und könnte in diesem aktuell hochdynamischen Technikfeld eine Rolle »ganz vorn« einnehmen. Und zwar nicht nur bei der Nutzung selbst, sondern auch bei der Berücksichtigung und vor allem der Umsetzung digitaler Souveränität in diesem Kontext. Dies kann auch dazu beitragen, insbesondere die oft noch zögernden kleinen und mittleren Unternehmen zu motivieren, sich gezielt mit der Technik an sich und mit entsprechenden Aspekten digitaler Souveränität auseinanderzusetzen.

Es ist daher sinnvoll, eine Bestandaufnahme von laufenden, konkreten Maßnahmen – z. B. von Realisierungsprojekten – auf allen staatlichen Ebenen zu machen, die digitale Souveränität im Kontext LLM-basierter KI-Lösungen fördern. Ausgehend von den drei identifizierten strategischen Zielen hat der IT-Planungsrat acht Lösungsansätze formuliert und jedem Lösungsansatz abstrakte Maßnahmen zu seiner Umsetzung zugeordnet:

1. **Vorausschauende Analyse und Steuerung:**
   - Strategische Marktanalysen
   - Strategische Indikatoren für Lagebild digitale Souveränität
2. **Beschaffung/Entwicklung alternativer IT-Lösungen:**
   - [Landkarte der] Machbarkeitsnachweise
   - [Durchführung von] Proofs of Concept (PoC)
   - [Förderung von] OSS-Alternativlösungen
3. **Herstellerunabhängige Modularität, (offene) Standards und Schnittstellen in der IT:**
   - Deutsche-Verwaltungscloud-Strategie[: herstellerunabhängige, modulare Architekturen sowie Ebenen übergreifende offene Standards und Schnittstellen]
   - [Weitere] technische Zielarchitekturen
4. **Aufbau digitaler Kompetenzen und Expertenwissen:**
   - [Austausch zu] vergleichbare[n] Vorhaben
   - Austausch mit Experten und Technologieanbietern
   - Kompetenzaufbau im Umfeld der Digitalisierung
5. **Kooperative Mitgestaltung von IT-Lösungen:**
   - Zentrales Code Repository für die öffentliche Verwaltung
   - Zusammenarbeitsmodelle Verwaltungsträger
   - Zusammenarbeitsmodelle OSS-Markt und -Communities
   - Zusammenarbeitsmodelle proprietärer Anbieter
6. **Gemeinsames Verständnis und Vorgehen:**
   - Strategie der öffentlichen Verwaltung
   - Arbeitsstruktur [in der AG Cloud Computing und Digitale Souveränität]
   - Zentrale Informationsplattform [zur Förderung der Vernetzung zwischen Akteuren sowie zur Information und zur Sensibilisierung über digitale Souveränität]
7. **Rechtliche Vorgaben:**
   - Anforderungen an Anbieter und Lösungen
   - Leitfäden für Beschaffung
   - Zentrale Beschaffungswege[: Identifikation und Sicherstellung von Möglichkeiten zur zentralen Beschaffung]
8. **Politische Steuerung**:
   - Gemeinsame Ziele und Initiativen auf EU-Ebene

In einem ersten Schritt soll sich exemplarisch angeschaut werden, inwieweit die genannten Lösungsansätze und Maßnahmen im Kontext KI (und idealerweise LLMs) von Relevanz sind beziehungsweise welche Ausprägungsform sie annehmen.

Die (1) vorausschauende Analyse und Steuerung von Abhängigkeiten ist originär innerhalb jeder einzelnen Institution notwendig, es kann aber sinnvoll sein, dies institutionsübergreifend für größere Betrachtungseinheiten mit einer annähernd einheitlichen Situation durchzuführen. Analyse und Steuerung müssen die jeweilige Institution umfassend in den Blick nehmen und somit auch die Besonderheiten, die der Einsatz LLM-basierter KI-Lösungen mit sich bringt, berücksichtigen. Es müssen Kriterien, Indikatoren und Konzepte identifiziert bzw. entwickelt werden, die eine konsistente Bewertung der Abhängigkeiten im zeitlichen Verlauf ermöglichen. Dazu will diese Studie beitragen.

Strategische Marktanalysen sollten sich stets auf eine konkrete Produkt- oder Komponentenkategorie – bestenfalls weiter konkretisiert durch z. B. Qualitäts-, Leistungs- oder Sicherheitsanforderungen – beziehen und in angemessenen (ausreichend kurzen) Abständen stattfinden, auch dann, wenn das strategische Ziel *Wechselmöglichkeit* aktuell als ausreichend gesichert betrachtet wird. Sie dienen der Identifikation (absehbar) verfügbarer Alternativen und der sich aus ihnen ergebenden Abhängigkeiten. Produkte im Kontext dieser Studie könnten beispielsweise »fertige« LLM-basierte KI-Lösungen sein, die auf Servern der Institution betrieben werden können. Eine Komponentenkategorie wären LLMs, die ganz bestimmte Schnittstellen besitzen, um sie in eigene Lösungen einbinden zu können. Derartige Analysen müssen stets auch etwaige technisch bedingte Abhängigkeiten berücksichtigen, die sich durch den Einsatz der betrachteten Produkte oder Komponenten in anderen Komponentenclustern ergeben können: Im Fall institutionsintern betriebener LLMs ist beispielsweise besonders an den bereits erörterten Bedarf von Rechenleistung zu denken.

Daran schließen auch die beiden folgenden Punkte an. Die Lösungsansätze (2) Beschaffung und Entwicklung alternativer IT-Lösungen und (3) herstellerunabhängige Modularität, (offene) Standards und Schnittstellen der IT lassen sich hier insofern gemeinsam erörtern, als dass sie in Bezug auf LLMs ähnliche Maßnahmen erfordern. So könnte die Entwicklung eines eigenen Sprachmodells (für die Verwaltung) als Alternative zu kommerziellen Anbietern angedacht werden. Mindestens sollten jedoch die konsequente Nutzung von Open-Source-Alternativen gestärkt und durch Nachnutzungsmöglichkeiten Entwicklungen und Umsetzungserfolge schnell geteilt werden. Darüber hinaus kann die Schaffung von Plattformen, die modular und standardisiert die Anbindung verschiedener Anwendungen, Sprachmodelle und Datenbestände ermöglichen, auf die Reduzierung von langfristigen Hersteller- und Produktabhängigkeiten einzahlen.

Vernetzt werden muss auch die Expertise, (4) zwecks Aufbau digitaler Kompetenzen und Expertenwissen. Die Anforderung organisierter und vernetzter Expertise in Bezug auf KI insgesamt ist auch ein wesentlicher Bestandteil der europäischen KI-VO. Kenntnisse und Fähigkeiten müssen aber sowohl auf die technischen Besonderheiten von LLMs hin angepasst werden als auch die Besonderheiten ihres Einsatzes in der öffentlichen Verwaltung berücksichtigen.

Die Maßnahmen zur (5) kooperativen Mitgestaltung von IT-Lösungen schließen mehrere Ebenen der Kooperation und des Dialoges ein: zwischen den Verwaltungsträgern sowie mit der Industrie und mit nichtindustriellen Bereitstellern. Eine Bereitstellung von Code in einem zentralen Code-Repository (opencode.de) könnte sich nicht nur positiv auf Nachnutzungsgelegenheiten auswirken, sondern erhöht auch die (verwaltungsinterne/teilöffentliche/öffentliche) Transparenz der eingesetzten Lösungen und berührt damit eine zentrale Herausforderung des KI-Einsatzes in der Verwaltung.

4.2 Umgesetzte Maßnahmen mit behördenübergreifendem Fokus

Von den laufenden Maßnahmen mit behördenübergreifendem Fokus, die auf die Erreichung der strategischen Ziele einzahlen können und bereits Erfolg versprechende Ergebnisse zeigen, sind die folgenden hervorzuheben:

BeKI

Das »Beratungszentrum für Künstliche Intelligenz« (BeKI) wird eine zentrale Anlauf- und Koordinierungsstelle für KI-Vorhaben in der Bundesverwaltung mit dem Ziel, ein koordiniertes Vorgehen bei der Nutzung von KI-Technologien und dem Aufbau entsprechender Infrastrukturen auf Bundesebene sicherzustellen. (CIO Bund 2023) »*Das BeKI soll der Bundesverwaltung Expertise zur verantwortungsvollen Nutzung von KI in Form eines Beratungsangebots zur Verfügung stellen, gezielt den sektor- und ebenenübergreifenden Austausch und die Vernetzung relevanter Stakeholder fördern sowie zukünftig zu Fortbildungsmaßnamen zu KI beraten und deren (Weiter-)Entwicklung anstoßen.*« (Deutscher Bundestag 2024)

BeKI sammelt, organisiert und vernetzt Kompetenzen und Wissen, forscht, entwickelt und produziert aber nicht selbst. Es zahlt somit auf die Wissens-, Transparenz- und Nutzungssouveränität ein. Zusammenarbeiten soll das BeKI besonders auch mit dem KIPITZ und dem »Kompetenzzentrum Künstliche Intelligenz« (beide s. unten).

ABOS

Die »Algorithmenbewertungsstelle für Organisationen und Behörden mit Sicherheitsaufgaben« (ABOS) *»soll die Unterstützung der Bundessicherheitsbehörden bei Fragen zu KI-Regulierung sowie qualitätsgesicherter und vertrauenswürdiger KI zentralisieren. Insbesondere soll die ABOS bei der Umsetzung der KI-Verordnung […] der EU im sicherheitsbehördlichen Bereich wichtige Aufgaben im Sinne eines Kompetenzzentrums übernehmen. Dies umfasst beispielsweise: Zentrale Beratung und Unterstützung für Sicherheitsbehörden des Bundes bezüglich der Umsetzung der KI-Verordnung sowie weiteren Themen zu KI-Regulierung und qualitätsgesicherter KI, Erstellung allgemeiner/zentraler Leitlinien und Frameworks für die Umsetzung der KI-Verordnung bei Sicherheitsbehörden des Bundes, Beobachtung von relevanten nationalen und internationalen Gremien zu KI-Regulierung, insbesondere einschlägige Standardisierungsgremien. Die ABOS soll daher nicht mit Plattformen oder nur zu spezifischen Plattformen arbeiten, sondern betrachtet die Anforderungen und die KI-Systeme der Sicherheitsbehörden individuell und ganzheitlich.«* (Deutscher Bundestag 2024)

MaKI

Das »Beratungszentrum für Künstliche Intelligenz« hat im Januar 2025 den »Marktplatz der KI-Möglichkeiten« (MaKI) zugänglich gemacht, der eine auf konkrete KI-Projekte bezogene Vernetzung der Bundesbehörden untereinander sowie mit potenziellen Kooperationspartnern und so Nachnutzungen und Kooperationen ermöglichen soll. Er bietet einen Überblick über vorhandene und geplante KI-Projekte.

Zweck ist der Austausch über KI-Projekte, Lösungen und Bedarfe. So soll dem Aufbau von Doppelstrukturen entgegengewirkt, gemeinsame Expertise aufgebaut und die Außendarstellung von KI in der Verwaltung und damit das Vertrauen in diese Verfahren gestärkt werden. Der Marktplatz adressiert besonders die Wissens- und die Betriebssouveränität und könnte auch zur Transparenzsouveränität beitragen. Er ist öV- und KI-spezifisch und kann sich perspektivisch aufgrund der Vielzahl von Projekten, die sich mit LLM-basierten KI-Lösungen beschäftigen, zu einer wichtigen Wissens- und Kooperationsdrehscheibe entwickeln.

Kompetenzzentrum Künstliche Intelligenz

Das bei der Bundesdruckerei angesiedelte »Kompetenzzentrum Künstliche Intelligenz« (vormals KI-KC) soll die Behörden der Bundesverwaltung technisch unterstützen, indem es projektbezogen berät und als »Entwicklungs- und Umsetzungshub« für KI-Prototypen die Erstellung von Proofs-of-Value umsetzt. Die Aufgaben lassen sich nicht vollständig von denen des BeKI abgrenzen, neben dem Aufbau von Expertise scheint hier aber deutlich stärkerer Anwendungsbezug gegeben zu sein, für einen Vergleich siehe Tabelle 2.

	BeKI	KI-KC
Anspruch	Beratungs- und Kompetenzzentrum sowie Vernetzungsplattform für den Einsatz von KI in der öffentlichen Verwaltung	KI-Entwicklungs- und Umsetzungshub für KI-Prototypen in der Bundesverwaltung
Tätigkeitsfelder	– Beratung (ethisch, technisch) – Vernetzung – Kompetenzaufbau – Wissensmanagement – Koordinierung übergreifender KI-Themen	– Entwicklung von Proof-of-Values (PoV)/Sandboxing – Beschleunigte Umsetzung von KI-Prototypen für die Bundesverwaltung innerhalb von Datenprojekten – Konkrete, projektbezogene Beratung im Rahmen der PoV

Tabelle 2: Vergleich BeKI und KI-KC (aus Deutscher Bundestag 2024)

KIPITZ

Durch das »KI-Portal des ITZBund« (KIPITZ) soll im Sinne des Einer-für-Alle-Prinzips eine hochgradig modularisierte und standardisierte Plattform zum Betrieb von LLMs in der Verwaltung geschaffen werden (ITZBund 2024). Es erlaubt den Betrieb großer Sprachmodelle auf Serverumgebungen des ITZBund ebenso wie die Anbindung von extern gehosteten Modellen. Das trägt zu Souveränitätsgewinnen auf der Ebene der Daten und der Software bei, die vollständig im ITZBund-Rechenzentrum verarbeitet und betrieben werden können. Die modulare Architektur der KIPITZ-Plattform soll die Anbindung unterschiedlichster Modelle unkompliziert möglich machen. Das KIPITZ kann damit in besonderer Weise zum souveränen Betrieb von LLMs in der Bundesverwaltung beitragen:

Die vorgesehene Client-Server-Infrastruktur soll die einzelnen Behörden von der Notwendigkeit entlasten, eine eigene

kostspielige, zeitweilig unausgelastete und schnell veraltende Server-Infrastruktur schaffen zu müssen oder diesbezüglich auf die Services von Drittanbietern angewiesen zu sein. Dies soll Synergien nicht nur für die Entwicklung und Anwendung von LLMs freisetzen, sondern auch eine gemeinsame strategische Planung erlauben, was dabei helfen kann, Abhängigkeiten vorausschauend zu steuern.

Das KIPITZ ist wohl im Hinblick auf die Souveränitätsdimensionen der umfassendste Ansatz. Die Betriebssouveränität wird durch den Aufbau zentraler, leistungsfähiger Rechenzentren gestärkt, das »Nadelöhr« Rechenleistung zwar nicht völlig gelöst, aber entschärft. Die Wissens- und Transparenzsouveränität kann durch die zentrale Organisation von Expertise gestärkt werden. Es wird betont, dass KIPITZ besonders für Open-Source-LLMs eine Plattform bieten kann. Das Projekt ist spezifisch auf die Nutzung von LLMs ausgerichtet und somit die Maßnahme, die am konkretesten die digitale Souveränität der öffentlichen Verwaltung im Hinblick auf LLMs adressiert.

Umsetzung der EU-Verordnung über künstliche Intelligenz

Die EU-Verordnung über künstliche Intelligenz (Verordnung (EU) 2024/1689) ist selbst keine Maßnahme, schreibt aber bestimmte Maßnahmen vor, die sich auch auf die digitale Souveränität auswirken. Dabei adressiert sie nicht explizit die öffentliche Verwaltung, als Betreiberin von (LLM-basierten) KI-Lösungen ist die öV aber in den Geltungsbereich eingeschlossen. Ferner unterliegen Drittanbieter, deren Dienstleistungen die öffentliche Verwaltung nutzt, der Verordnung.

Die Verordnung legt fest, dass (a) Expertise aufgebaut, (b) Risikoeinschätzungen für die jeweiligen Anwendungsfälle vorgenommen und (c) öffentlich zugängliche Transparenzregister eingeführt werden müssen.

Zur übergreifenden Stärkung der digitalen Souveränität können vor allem zwei Vorgaben der Verordnung beitragen:

1. Die Einrichtung nationaler und europäischer Gremien, die Kompetenzen und Wissen, auch über die Modalitäten der KI-Wertschöpfungskette, aufbauen sollen (vgl. Art. 66, Abs. e, vi), stärkt primär die Wissenssouveränität.
2. Die Schaffung von Transparenzregistern zahlt auf die Wissens- und die Betriebssouveränität ein, etwa durch das Offenlegen von Wertschöpfungsketten und Best Practices.

Beides erfordert Maßnahmen der öffentlichen Verwaltung, allerdings nicht in einer der im Kontext digitaler Souveränität betrachteten Rollen (Nutzende, Betreiber, Beschaffer), sondern in der originären Rolle des Gesetzesvollzuges. Nichtsdestotrotz wird die zentrale Umsetzung der Transparenzregister durch die Bundesverwaltung (geplant über den »Marktplatz der KI-Möglichkeiten« (MaKI) bzw. die »Algorithmenbewertungsstelle für Behörden und Organisationen mit Sicherheitsaufgaben« (ABOS)) die Möglichkeiten der öffentlichen Institutionen stärken, sich zu informieren und Austausch- und Kooperationspartner zu identifizieren, wenn die Daten der Register entsprechend zugänglich gemacht werden (was allerdings bzgl. der beim ABOS verwalteten Daten nur ein sehr kleiner, geschlossener Kreis von Institutionen sein wird).

5. Spannungsfelder der Digitalen Souveränität im Ausland

Digitale Souveränität etabliert sich auch im internationalen Kontext als strategisches Leitprinzip der Verwaltungsdigitalisierung – doch die Verwaltungen der meisten Staaten können auf keine nationalen Anbieter zurückgreifen, die die Angebote der Hyperscaler ersetzen können. So besteht ein wachsender Trade-off zwischen Souveränität und LLM-Nutzung. Dieser Abschnitt analysiert die verschiedenen Strategien, mit denen Staaten diesen Trade-off navigieren.

Die Analyse stützt sich auf zwei zentrale Quellen: auf eine vergleichende Auswertung nationaler und multinationaler KI- sowie Digitalisierungsstrategien und auf Expert:inneninterviews mit staatlichen und akademischen Akteur:innen aus dem Feld der Verwaltungsdigitalisierung und staatlichen KI-Nutzung, darunter auch Personen, die an der Ausarbeitung entsprechender Strategien beteiligt waren. Der Länderauswahl liegt der AI Readiness Index von Oxford Insights zugrunde (oxfordinsights 2024). Untersucht wurden die 22 höchstplatzierten Staaten (die führenden Modellentwickler, USA und China, sind ausgenommen). Dies gewährleistet eine starke Abdeckung europäischer Länder in mit Deutschland vergleichbaren Positionen. Eine vollständige Auflistung der Länder und analysierten Dokumente findet sich im Anhang A.3, die ausführliche Analyse findet sich im Anhang A.4.

5.1 Entwicklung des digitalen Souveränitätsverständnisses seit 2020

Digitale Souveränität gewinnt vor allem seit gut zwei Jahren an politischer Aufmerksamkeit, wird jedoch schon länger in Strategien berücksichtigt. So betont etwa die deutsche KI-Strategie von 2020 die Bedeutung digitaler Souveränität und verweist auf Initiativen wie GAIA-X, ohne jedoch konkrete Vorgaben für die Nutzung souveräner KI-Infrastrukturen im Verwaltungshandeln zu formulieren. Auch Frankreich rückt in seiner nationalen KI-Strategie (2021–2025) das Ziel technologischer Eigenständigkeit in den Mittelpunkt, doch bleibt die Anbindung an operative Verwaltungsprozesse bislang weitgehend aus.

Die gestiegene Relevanz digitaler Souveränität in Digitalisierungsstrategien ist nicht zuletzt auf das Ergebnis der Präsidentenwahl in den USA zurückzuführen. Die Nutzung amerikanischer Hyperscaler, vor allem im Bereich Cloud Computing, wurde in der Vergangenheit häufig als bekanntes und durch technische oder vertragliche Maßnahmen beherrschbares Risiko eingeschätzt. Diese Perspektive hat sich jedoch verändert. In mehreren Interviews wurde deutlich, dass politische Entwicklungen in den USA als unmittelbar sicherheitsrelevant für zentrale IT-Infrastrukturen in Europa wahrgenommen werden. Verwaltungsakteur:innen betonten, dass etwaige Veränderungen in der US-Regierung direkten Einfluss auf die Nutzbarkeit, Stabilität und rechtliche Absicherung digitaler Dienste haben können. Damit wird digitale Souveränität nicht nur als langfristiges strategisches Ziel, sondern zunehmend auch als Voraussetzung für kurzfristige Handlungsfähigkeit verstanden.

Auch im öffentlichen Sektor der USA selbst wird seit dem Regierungswechsel eine deutlich aggressivere KI-Strategie verfolgt. In Dokumenten wie dem OMB Memorandum M-24-10 (Office of Management and Budget 2024) werden Bundesbehörden angehalten, mögliche KI-Anwendungsfälle zu erkennen, strukturiert aufzunehmen und umzusetzen. Die Ambition und der Umfang dieser Anforderungen sind hoch und zeigen einen starken Fokus auf die schnelle und umfassende Automatisierung von Verwaltungsaufgaben durch Nutzung von Künstlicher Intelligenz.

Diese gepaarten Entwicklungen lösen in vielen Staaten eine neue Evaluation von Abhängigkeiten in staatlicher digitaler Infrastruktur aus, welche nicht auf die Betrachtung von LLMs begrenzt ist. Tatsächlich wird der Umgang mit großen Sprachmodellen bislang nur vereinzelt in bestehenden Digitalisierungsstrategien adressiert. Ihre starke Verflechtung mit Hyperscaler-Infrastruktur – insbesondere durch API-basierte Nutzung über Plattformen wie Azure – erschwert eine unabhängige Governance. Der Fokus dieses Abschnitts sind deswegen nicht nur staatliche Digitalisierungsstrategien, sondern auch sektorübergreifende KI-Strategien.

5.2 Trade-off zwischen digitaler Souveränität und staatlicher Kapazität

Digitale Souveränität wird im Großteil der analysierten Strategiedokumente als strategisches Ziel erwähnt, wird jedoch meist in einem engen Sinne verstanden: Im Vordergrund steht die Reduktion technologischer Abhängigkeiten von ausländischen Anbietern, insbesondere US-amerikanischen Hyperscalern. Die grundlegende infrastrukturelle Abhängigkeit von privatwirtschaftlich kontrollierten Technologien, insbesondere im Bereich des Cloud Computing, wird dagegen nur selten als eigenständiges Governance-Problem adressiert. Gleichzeitig verfügen viele Staaten über keine eigenständig entwickelte oder europäisch abgestimmte Alternative, die in Funktionalität und Skalierbarkeit mit den Angeboten internationaler Marktführer konkurrieren könnte.

So zeigt sich ein wiederkehrendes Spannungsfeld: Der Wunsch nach technologischer Kontrolle kollidiert mit dem unmittelbaren Bedarf nach funktionalem Kapazitätsgewinn – ein Zielkonflikt, der bislang nur in wenigen Staaten systematisch aufgelöst wird.

Im internationalen Vergleich lassen sich fünf Strategiemuster im Umgang mit diesem Spannungsverhältnis zwischen digitaler Souveränität und staatlicher Kapazität identifizieren. Diese Ansätze – konservativ, balanciert, pragmatisch, investitionsorientiert und offensiv – unterscheiden sich in der Gewichtung von Kontrollanspruch, Risikobereitschaft und Investitionsbereitschaft. Die ausführlichen Ergebnisse der Analyse finden sich im Anhang A.4

Konservativ

Staaten mit einem konservativen Ansatz priorisieren die Integrität staatlicher Prozesse, Datenschutz und institutionelle Kontrolle gegenüber potenziellen Effizienzgewinnen durch generative KI. Der Einsatz von LLMs wird hier als Risiko für Prozessgerechtigkeit und demokratische Rechenschaftspflicht betrachtet, insbesondere aufgrund der Intransparenz vieler LLMs Intransparenz und der häufigen Abhängigkeit von externen, kommerziellen Anbietern. Zwar wird die digitale Souveränität selten explizit als Ziel formuliert, doch ergeben sich aus dem Bedürfnis nach rechtlicher Nachvollziehbarkeit, normativer Konsistenz und Datenschutz häufig Maßnahmen, die faktisch souveräne Infrastrukturen begünstigen. Dazu zählen etwa restriktive Regelungen zur API-Nutzung, Anforderungen an Open-Source-Nachvollziehbarkeit oder der Aufbau nationaler Daten- und Modellregister. 2 (Österreich, Italien) von 22 Ländern verfolgen einen konservativen Ansatz.

Beispiel: Italien
Die Italienische Nationale KI-Strategie 2024–2026 (Dipartimento per la transformazione digitale 2024) positioniert sich explizit gegen eine unkritische Übernahme generativer Systeme aus dem Ausland und hebt mehrfach die Risiken »kultureller Homogenisierung«, technologischer Abhängigkeiten und strategischer Kontrollverluste hervor. Im Zentrum der Strategie steht das Ziel, KI-Lösungen zu entwickeln, die die spezifischen Werte, kulturellen Eigenheiten und rechtlichen Normen des italienischen Systems reflektieren. Das Papier warnt explizit vor einem Import ausländischer generativer Modelle, die »Ideen und Werte reproduzieren, die oft nicht mit dem italienischen oder europäischen Kontext übereinstimmen«, was langfristig zu einer »kulturellen Stereotypisierung« führen könne.

Balanciert

Staaten mit einem balancierten Ansatz verfolgen eine Strategie, die zwischen technologischer Offenheit und struktureller Vorsicht vermittelt. Der Einsatz von LLMs und generativer KI wird grundsätzlich begrüßt, aber unter klaren Auflagen: Es werden sowohl die Chancen für Effizienz und Innovation erkannt als auch die Risiken für Datenschutz, Anbieterabhängigkeit und normative Kohärenz ernst genommen. In vielen Fällen ist ein balancierter Ansatz das Ergebnis einer bislang nicht auf LLMs fokussierten Digitalisierungsstrategie. 7 (Finnland, Frankreich, Japan, Niederlande, Norwegen, Schweden, UK) von 22 Ländern verfolgen einen balancierten Ansatz.

Beispiel: Frankreich
Frankreich verfolgt mit der nationalen KI-Strategie (Gouvernement 2021) einen doppelten Kurs: Einerseits wird in nationale Recheninfrastruktur, öffentliche Supercomputer (z. B. Jean Zay), lokale Cloud-Anbieter und Souveränitätsprojekte wie Mistral AI investiert. Andererseits arbeitet Frankreich gezielt mit globalen Technologieanbietern zusammen, etwa über Forschungscluster und Großprojekte zur Entwicklung französischsprachiger LLMs in Kooperation mit öffentlichen Dateninstituten wie der Bibliothèque nationale de France (BnF) und dem Institut national de l'audiovisuel (INA). Gleichzeitig werden ethische Standards über Governance-Strukturen wie das geplante nationale Evaluationsinstitut für KI abgesichert.

Pragmatisch

Staaten mit einem pragmatischen Ansatz verfolgen einen stark nutzenorientierten Zugang zum Einsatz von LLMs im öffentlichen Sektor. Im Vordergrund stehen Effizienzgewinne, bessere Servicequalität und Innovationsfähigkeit, auch auf Kosten der technologischen Souveränität oder strategischen Unabhängigkeit. Der Einsatz marktverfügbarer, auch nicht-souveräner Lösungen wird dabei nicht als strukturelles Problem betrachtet, solange er sich innerhalb regulatorischer und ethischer Leitplanken bewegt. 3 (Australien, Kanada, Irland) von 22 Ländern verfolgen einen pragmatischen Ansatz.

Beispiel: Australien
Australien exemplifiziert mit seinem National Framework for the Assurance of AI in Government (Australian Government 2024) einen risikobasierten, technologieoffenen Rahmen zur Integration von KI im öffentlichen Sektor. Die technische oder institutionelle Eigenentwicklung souveräner LLMs spielt keine zentrale Rolle. Vielmehr setzt Australien auf transparente Prozesse, verantwortungsvolle Datenverwendung (z. B. über die SURE-Plattform für datenschutzgerechten Zugang zu Gesundheits- und Verwaltungsdaten) und adaptive Governance-Strukturen. Das Dokument beschreibt KI primär als Werkzeug zur Optimierung bestehender Verwaltungsprozesse statt als geopolitisch relevante Infrastruktur.

Investitionsorientiert

Der investitionsorientierte Ansatz zielt auf den strategischen und langfristigen Aufbau souveräner Kapazitäten im Umgang mit LLMs – entweder durch eigene Modellentwicklung oder durch staatlich kontrollierte Infrastrukturen, die den sicheren und kontextgerechten Einsatz auch externer Modelle ermöglichen. Der Fokus liegt auf der aktiven Gestaltung der technischen, institutionellen und organisatorischen Voraussetzungen für eine vertrauenswürdige KI-Nutzung im öffentlichen Sektor. Somit ist das investitionsorientierte Modell nicht zwingend auf vollständige Eigenentwicklung angewiesen. Deutschland und 6 (Belgien, Dänemark, Estland, Malaysia, Südkorea, Taiwan) weitere von 22 Ländern verfolgen einen Investitionsorientierten Ansatz.

Beispiel: Estland
Estland investiert in seiner nationalen KI-Strategie 2024–2026 (Teadusministeerium et al. 2024) gezielt in eigene Systeme, digitale Plattformen wie X-Road sowie sektorübergreifende Datennutzung, um langfristige technologische Unabhängigkeit zu sichern. Die Strategie betont die Notwendigkeit vertrauenswürdiger, an den estnischen Rechts- und Verwaltungsrahmen angepasster Lösungen und sieht öffentliche Innovationsförderung, Ausbildung und Forschungskooperationen als zentrale Hebel. Die souveräne Modellkontrolle wird hier primär über staatlich koordinierte Entwicklung und Infrastruktur realisiert.

Offensiv

Staaten mit einem offensiven Ansatz begegnen der Einführung von LLMs mit gezielter Ambition, über den öffentlichen Sektor hinaus international technologische Führungspositionen zu erlangen. Der Trade-off wird durch den aggressiven Aufbau eigener Modelle und Grundkapazitäten entlang der gesamten Wertschöpfungskette gelöst. Diese angestrebte Positionierung ist stark investitionsabhängig und wird entsprechend nur von wirtschaftlich starken Ländern verfolgt. Sie ist verbunden mit einer hohen Risikobereitschaft, pragmatischer Regulierung und dem Aufbau öffentlich-privater Ökosysteme. Die Governance erfolgt häufig ex-post oder begleitend. 3 (Saudi-Arabien, Singapur, VAE) von 22 Ländern verfolgen einen offensiven Ansatz.

Beispiel: Saudi-Arabien
Saudi-Arabien verfolgt mit der National Strategy for Data and AI (SDAIA 2020) einen ambitionierten Ansatz: Das Land will zu einem globalen Zentrum für Daten- und KI-Innovation werden, gestützt auf massive staatliche Investitionen, strategische Großprojekte (z. B. NEOM) und zentralisierte Steuerung über die Saudi Data & AI Authority (SDAIA). Künstliche Intelligenz wird als transformatives Element der wirtschaftlichen Diversifikation im Rahmen von »Vision 2030« verstanden. Der Aufbau eines nationalen Datenbanksystems und von KI-Forschungszentren sowie die Durchführung globaler Events (z. B. Global AI Summit) unterstreichen den geopolitisch motivierten Anspruch, selber Produzent von führenden Foundation Models zu werden.

Beispiel: Singapur
Singapur setzt mit der National AI Strategy 2.0 (Government of Singapore 2023) auf ein umfassendes Systemdesign zur Beschleunigung von KI-Innovation und -Einsatz in allen Sektoren, insbesondere im öffentlichen Bereich. Die Strategie sieht Singapur als »Global Hub« für verantwortungsvolle KI-Nutzung, sowie als »Test Bed« für neue Anwendungen. Es wird gezielt in Rechenkapazitäten, Talente, sektorale Anwendungszentren (»Centres of Excellence«) und offene Innovationsplattformen investiert. Zugleich wird mit globalen Akteuren wie Google kooperiert (z. B. »AI Trailblazers«), um rasch neue Use Cases zu entwickeln. Durch gezielte Vorwärtsintegration in internationale Innovationsnetzwerke will Singapur trotz begrenzter Ressourcen eine führende Rolle in der globalen KI-Wertschöpfung einnehmen.

6. Digitale Souveränität von LLM-Projekten der Bundesverwaltung

Nachdem im vorigen Abschnitt »top-down« die Maßnahmen in Deutschland und im Ausland zu digitaler Souveränität betrachtet wurden, werden In diesem Abschnitt die empirischen, »bottom-up« gewonnenen Ergebnisse zu den LLM-Projekten in der Bundesverwaltung vorgestellt. Dafür wird zuerst die dafür entwickelte Indikatorik vorgestellt und die daraus resultierende Matrix zur Bewertung beschrieben. Auf dieser Basis werden Rückschlüsse auf existierende und zukünftige Probleme hinsichtlich der digitalen Souveränität (auch »Schmerzpunkte« genannt) getroffen.

6.1 Indikatorik

Wie in Abschnitt 2 beschrieben, wurden die für die Erhebung genutzten Indikatoren auf Basis einer Literaturrecherche und durch Einbindung von Expertinnen und Experten erstellt. Alle insgesamt 21 Indikatoren mit Beschreibung und Ausprägungsstufen sind in Tabelle 3 aufgelistet und finden sich ausführlich beschrieben in Anhang A.5. Sie sind jeweils einem der strategischen Ziele digitaler Souveränität (*Wechselmöglichkeit*, *Gestaltungsfähigkeit*, *Einfluss auf Anbieter*) zugeordnet und zahlen auf jeweils eine oder mehrere Betrachtungsebenen ein, sodass sich eine Matrix zwischen Betrachtungsebene und Ziel aufspannt. Während die strategischen Ziele in Abschnitt 1.1 bereits ausführlich besprochen wurden, werden die Betrachtungsebenen im Folgenden näher erläutert.

Die Trennung in mehrere Ebenen erscheint sinnvoll, da moderne digitale Anwendungen in ein ganzes Netz technischer Abhängigkeiten eingebettet sind. Das ist bei LLM-Systemen nicht anders. ChatGPT über den Browser eine Frage zu stellen, setzt eine Kette von Aktionen in Gang, die über verteilte Systeme und Hardware einen Informationsfluss der Eingabedaten vom Nutzenden zum LLM und dessen Ausgabe zurück ermöglicht. Die zur Erfüllung dieses Prozesses nötigen Komponenten lassen sich – wie auch in Abschnitt 1.1 beschrieben – als ein Technologie-Bündel betrachten (Mohabbat Kar und Thapa 2020) und umfassen Hardware, (vernetzte) Software, dabei insbesondere das LLM, und Daten.

Die erste Betrachtungsebene fokussiert auf die **verwendeten Daten**. Darunter fallen alle Daten, die im Rahmen einer öV-spezifischen Anwendung erforderlich sind. Dies können zum Beispiel Daten sein, die für ein Feintuning eines LLMs verwendet werden, oder auch die Daten einer Wissensbasis, die für Retrieval Augmented Generation (RAG) genutzt werden. Es sind also die Daten, die wesentlich dafür sind, dass ein LLM für eine

Wechselmöglichkeit	Gestaltungsfähigkeit	Einfluss auf Anbieter
Modularität	Softwaredokumentation	Geschlossene Ökosysteme
Nachnutzbarkeit	Technische Kompetenzen	Rechtliche Kompetenzen
Open Source	Austausch und gegenseitiges Lernen	Zertifizierungen
Anzahl alternativer Modelle	Informationsbereitstellung	Verhandlungsmacht
Flexible Modellwahl	Open-Source-Modell	Sitz des Anbieters
Cloud vs. On-Premise	Zusammenarbeitsstrukturen	Standort/Anbieter der Cloudserver
Dateiformate	Datenquellen & Verfügbarkeit	
Cloud LLM	Datenanpassbarkeit	

Tabelle 3: Indikatoren digitale Souveränität

fachspezifische Anwendung tatsächlich nützlich sein kann. Nicht betrachtet werden die Daten, die für das Pre-Training eines LLMs genutzt wurden.

Die zweite Betrachtungsebene ist die genutzte Infrastruktur. Diese umfasst Strukturen und Hardware, die **den Betrieb** eines LLM-Systems ermöglichen. Dabei wird vor allem zwischen on-premise Lösungen und (public) Cloudlösungen unterschieden. LLM-Systeme sind häufig verteilte Systeme, da das LLM und die restliche Anwendung oftmals getrennt sind und über APIs miteinander kommunizieren.

Auf der dritten Betrachtungsebene geht es um **die LLMs**, die genutzt werden. Dabei ist LLM als (vor-)trainiertes statistisches Modell zur Generierung von Text definiert. Bekannte Beispiele hierfür sind GPT-4, Llama, Claude und Mistral. Neben der Informationsbereitstellung der Anbieter interessiert aus der Perspektive der digitalen Souveränität vor allem die Frage nach der Offenheit des Modells. Dabei handelt es sich um keine binäre Kategorie, stattdessen eröffnet sich hier ein Spektrum, das in Abschnitt 3.2 diskutiert wurde.

Die vierte Betrachtungsebene ist **die Anwendung**, also die Software, in welche die LLMs eingebettet sind. Darunter fallen vor allem Frontend und Backend. Beim Frontend kann es sich zum Beispiel um eine dedizierte Benutzeroberfläche handeln, wie etwa bei ChatGPT, oder auch die Einbettung in bestehende Software, wie zum Beispiel bei Textbearbeitungssoftware oder E-Mail-Diensten.

Das beschriebene vierstufige Ebenenmodell hat nicht den Anspruch, dass die Ebenen disjunkt sind oder strikt aufeinander aufbauen. Die vorgenommene Unterteilung hilft jedoch, eine differenzierte Betrachtung digitaler Souveränität bei LLM-Systemen vorzunehmen und so Schmerzpunkte präziser identifizieren zu können.

Die Zusammensetzung der Bewertung innerhalb der Matrix ergibt sich als die durchschnittliche Bewertung der Projekte (insgesamt P Projekte) entlang der Indikatoren für die jeweiligen Matrixeinträge $(m_{i,j})$, im Kern also folgendermaßen:

$$(m_{i,j}) = \left((m_{i,j,1}, \dots, m_{i,j,P})\right) \mapsto \frac{100}{P} * \sum_{k=1}^{P} f(m_{i,j,k})$$

$$f: x \in \mathbb{N}^n \mapsto \sum_{i=0}^{n} \frac{x_i}{3n}$$

Jeder Indikator hat maximal vier Ausprägungsstufen mit dem Höchstwert 3, der damit gleichzeitig den maximal souveränen Zustand definiert. Die Funktion f summiert die Indikatorausprägungen eines Projektes für einen Matrixeintrag auf, teilt durch die Summe der Höchstwerte aller Indikatoren des Eintrages und berechnet so einen Score, der zwischen 0 und 1 liegt. Der Durchschnitt über die Scores aller Projekte ergibt den Matrixeintrag . Die Ergebnisse der Matrix auf Basis der erhobenen Daten werden im nächsten Abschnitt beschrieben.

6.2 Datenerhebung

Für die Erhebung wurden KI-Projekte innerhalb der Bundesverwaltung mit explizitem Bezug zu LLMs berücksichtigt. Als Ausgangsbasis dienten die im »Marktplatz der KI-Möglichkeiten« eingetragenen Projekte. Von insgesamt 85 angefragten Projekten erhielten wir 60, davon 40 vollständige Antworten, wobei insgesamt 33 tatsächlich LLMs nutzen und damit berücksichtigt worden sind. Weitere 20 Projekte wurden nach Absprache nicht erfasst, da sie sich noch in einem zu frühen Projektstadium befanden. Damit haben wir von mehr als zwei Drittel der Projekte Rückmeldung zur Erhebung erhalten. Alle vorgestellten Ergebnisse sollten unter der Prämisse beachtet werden, dass es sich um Selbsteinschätzungen der Projekte handelt.

Methodik	Online-Erhebungsbogen
Grundgesamtheit	KI-Projekte der Bundesverwaltung aus den Daten des »Marktplatz der KI-Möglichkeiten« (MaKI)
Relevante Projekte	KI-Projekte mit vermutlichem LLM-Bezug
Zielpersonen	Projektverantwortliche
Angefragte Projekte	n = 85
Rückmeldungen	n = 60
Rückmeldungen LLM-relevant und ausgefüllt	n = 33
Befragungszeitraum	13.02.2025 – 28.02.2025

Tabelle 4: Wesentliche Charakteristika der Erhebung zu KI-Projekten

6.3 Empirische Ausprägungen digitaler Souveränität in den Projekten

Bei den im Folgenden vorgestellten Ergebnissen der Erhebung und der anschließend von uns durchgeführten Auswertung mittels der vorgestellten Indikatoren handelt es sich nicht um ein abschließendes Bild zur digitalen Souveränität der Bundesverwaltung im Bereich von KI, sondern um die strukturierte Untersuchung von Chancen und sich möglicherweise abzeichnenden Risiken und Abhängigkeiten entlang aktuell laufender Projekte. Alle Projekte flossen in gleichem Maße in die Wertung mit ein, wobei in den Fällen, in denen vertiefende Interviews durchgeführt wurden, die Ergebnisse punktuell vertieft und kontextualisiert werden konnten.

6.3.1 Allgemeine Projektaspekte

Die betrachteten Projekte lassen sich grundsätzlich in zwei Gruppen aufteilen:

- In der Mehrzahl der Projekte ist der Einsatz von LLMs mit einer spezifischen Arbeitsunterstützung verbunden. Dies können beispielsweise ein automatisierter Abgleich von Fachinformationen, die Erstellung von Lageberichten oder Mustererkennung aus Fallbeschreibungen sein.
- In einigen wenigen Projekten ist das Ziel, ein allgemeineres Hilfswerkzeug für unterschiedliche Arten der Textarbeit bereitzustellen. Nutzende sollen mit diesen Werkzeugen beispielsweise eigene Dokumente hochladen, diese analysieren, zusammenfassen oder übersetzen lassen können, weitgehend unabhängig von dem Einsatzzweck der Ergebnisse.

Von den berücksichtigten Projekten sind etwas weniger als die Hälfte (15 Projekte) in Betrieb, etwa ein Drittel (10) in Entwicklung, sowie ähnlich viele (8 Projekte) in Ideenphase oder Planung. Dabei fiel es den Projekten mitunter schwer, sich klar in Betrieb oder Entwicklung zu verorten, da es sich um kontinuierliche Weiterentwicklungen handelt, während die Systeme bereits zur Nutzung bereitstehen. Manche (3 Projekte) gaben außerdem an, Proofs-of-Concept zu sein und sich in einer Testumgebung zu befinden.

Das Projektvolumen (in Euro) lieg bei einem Drittel (10 Projekte) zwischen 100.000 bis 1 Millionen Euro, bei einem weiteren knappen Drittel (8 Projekte) zwischen 10.000 bis 100.000 Euro. Vier weitere Projekte gaben ein Projektvolumen von 1 Mio. Euro und mehr an.

Ein zweigeteiltes Bild ergibt sich bei den Adressaten. Etwa die Hälfte der Projekte gab an, spezifische Referate zu adressieren, während die andere Hälfte das eigene Haus adressiert. Es gibt einige Projekte, die explizit ressortübergreifend angelegt sind (z. B. AIUTO) beziehungsweise die gesamte Bundesverwaltung adressieren (KIPITZ).

Die Erhebung zeigte, dass etwa drei Viertel (25 Projekte) vor oder während der Entwicklung in unterschiedlichen Formaten in einen Erfahrungsaustausch mit Projektexternen getreten sind. Das waren sowohl informelle als auch institutionalisierte Formate. Mehrfach wurde als Austauschpartner das ITZBund genannt. Das ist insbesondere im Hinblick auf das Ziel der *Gestaltungsfähigkeit* interessant, da ein Erfahrungsaustausch zu Zusammenarbeitsstrukturen für die (Weiter-)Entwicklung von IT-Lösungen führen kann. Es zeigte sich auch, dass zumeist zwar Kenntnis über die Projekte anderer Häuser herrscht, sich allerdings mehr (institutionalisierter) behördenübergreifender Austausch gewünscht wird. Aus den Interviews ergab sich auch, dass insbesondere Zeitmangel einer gewünschten Vertiefung des Austausches mit anderen entgegensteht.

Für das Ziel der *Gestaltungsfähigkeit* sind darüber hinaus ausreichende Kompetenzen entscheidend. Aus der Erhebung ergibt sich ein gemischtes Bild. Die Kompetenzen innerhalb der (Entwickler-)Teams werden als insgesamt gut eingeschätzt: Die fachliche Kompetenz gilt als gut (~8 von 10 Punkten). Etwas geringer, aber ebenfalls gut wird die technische Kompetenz eingeschätzt, allerdings mit einer höheren Varianz zwischen den Projekten. Das heißt, einzelne Projekte gaben an, über gar keine beziehungsweise sehr geringe technische Kompetenz zu verfügen. Ähnlich wird die KI-spezifische Kompetenz durchschnittlich eingeschätzt (~6 von 10 Punkten), allerdings noch einmal etwas schlechter als die rein technische. Die rechtlichen Kompetenzen werden noch etwas geringer eingeschätzt (~5 von 10 Punkten). Auch in anschließenden Interviews wurde betont, dass es hier Verbesserungspotenzial gibt. Gerade in dem dynamischen Feld der KI und dazugehöriger Regulatorik fällt es den Projektverantwortlichen teilweise schwer, Schritt zu halten. Wenn die Regularien als unklar empfunden werden und die rechtliche Expertise in den Teams gering ist, dann kann es zu Verzögerungen (bis zum Abbruch) von Projekten kommen.

In den Interviews mit den Projekten wurde bezüglich der Kompetenzen außerdem betont, dass größere Verbesserungsmöglichkeiten vor allem in den Digital- und KI-Kompetenzen der Nutzendengruppen innerhalb der Verwaltung gesehen werden. Für einen effektiven und sicheren Einsatz der entwickelten Systeme bräuchte es Kompetenzaufbau, der sich unmittelbar an den Systemen orientiert.

6.3.2 Software und Betrieb

Im Bereich von Software und Betrieb wurden in der Erhebung Fragen zur Anwendung, zu den verwendeten LLMs und den verwendeten Daten gestellt. Anwendung und LLM wurden in der Erhebung getrennt betrachtet. Die Anwendung ist die Software (bestehend aus Frontend und Backend) zwischen Mensch (Nutzer:in) und LLM. Bei Anwendungen kann es sich um Bürosoftware, Weboberflächen oder eigens entwickelte Dienste

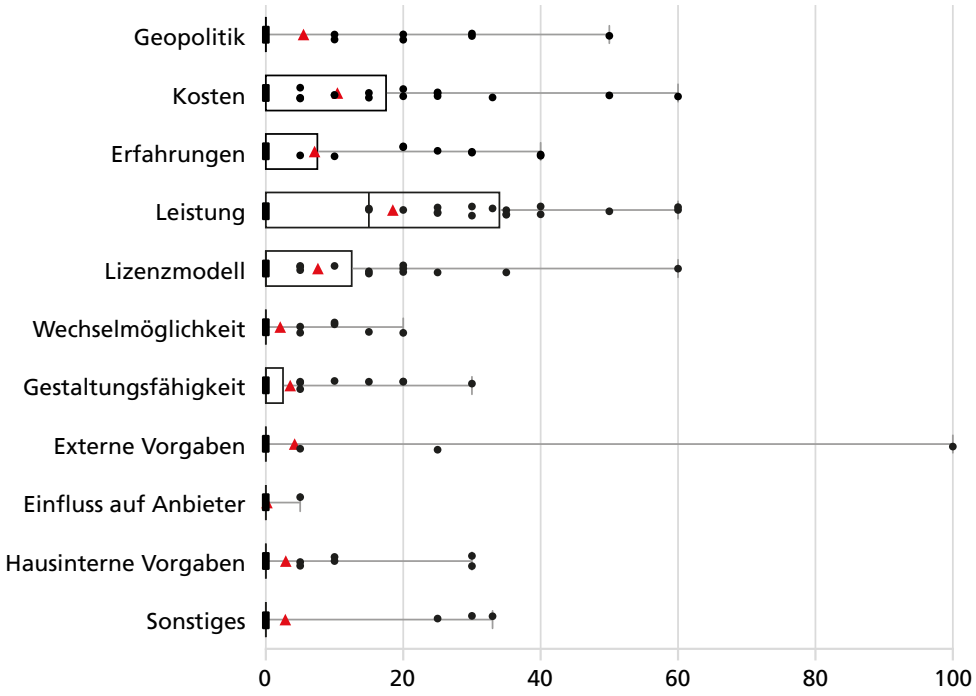
handeln. Sie kommunizieren über geeignete Schnittstellen mit einem oder mehreren LLMs, die ggf. auf anderen Servern laufen können. In der Erhebung war von Interesse, wie modular die Anwendung aufgebaut ist, ob Open Source genutzt wird, ob sie als Open Source bereitgestellt wird und wo sie betrieben wird. Für die LLMs wurde neben Fragen zur Wahlentscheidung ebenfalls die Betriebsart abgefragt.

In der Erhebung wurde nach den wichtigsten Kriterien der Projekte bei der Wahl eines geeigneten LLMs gefragt. Analog zur Gewichtung von Zuschlagskriterien bei einer Vergabe sollten 100 Punkte frei über alle Kriterien verteilt werden. Dabei zeigte sich, dass alle vorgeschlagenen 10 Kriterien (siehe Abbildung 6 und weiterführend Anhang A.1) von mindestens einem Projekt einmal angegeben sowie auch weitere genannt wurden. Aus Abbildung 6 lassen sich anhand der schwarzen Punkte die Angaben der Projekte und anhand der roten Dreiecke außerdem die durchschnittliche Punktzahl pro Kriterium ablesen.

Im Durchschnitt ist demnach für die Projekte das wichtigste Kriterium die Leistung (~20 Punkte), gefolgt von den Kosten (im Durchschnitt ~12 Punkte). *Wechselmöglichkeit*, *Gestaltungsfähigkeit* und *Einfluss auf Anbieter* als explizite Ziele digitaler Souveränität sind bei der Entscheidung eher weniger wichtig, werden aber teilweise berücksichtigt: Bei *Gestaltungsfähigkeit* gibt es vier Projekte, die Werte von 10–30 vergaben, immerhin drei Projekte bei *Wechselmöglichkeit*. *Einfluss auf Anbieter* hingegen ist durchgängig nicht relevant. Das ist allerdings noch kein klares Indiz für fehlende digitale Souveränität in diesem Bereich: Da die meisten Projekte auf Open-Source-Lösungen setzen, bei denen kein externer Anbieter genutzt wird, hat das Kriterium für viele Projekte in diesem Fall schlicht keine Relevanz.

Auch geopolitische Aspekte, obwohl relevant (6 Projekte vergaben mehr als zehn Punkte), treten im Mittel hinter Kosten und Leistung zurück. Hier wäre ein höherer Wert wünschenswert. So zeigt sich, dass eine Bevorzugung europäischer Lösungen auf der Ebene der Wahl von LLMs keine größere Rolle zu spielen scheint.

Unter sonstigen Kriterien wurde darüber hinaus »Ethik, Bias, Transparenz der Modelle, Energieverbrauch«, »Energieverbrauch, Robustheit, Transparenz« und »Vortraining auf relevanten Datensätzen« angegeben. Das zeigt, dass ein Bewusstsein über die ökologischen Auswirkungen von LLMs mindestens bei einzelnen Projekten mitgedacht wird und bei der Wahlentscheidung eine Rolle spielt. Wünschenswert wären hier höhere Werte, auch wenn diese nicht unmittelbar etwas mit digitaler Souveränität zu tun haben.



Vergabepunkte aller Projekte.
Das rote Dreieck markiert die entsprechenden Mittelwerte

Abbildung 6: Kriterien der LLM-Wahl

Bei dem Betrieb zeichnet sich eine klare Tendenz zum Eigenbetrieb sowohl der Anwendung als auch des LLMs ab. Die Anwendung läuft bei über der Hälfte (22 Projekte) lokal, auch das LLM wird bei knapp der Hälfte (17 Projekte) lokal betrieben. Teilweise wird für beides ein IT-Dienstleister beauftragt (5 Projekte), in weiteren Fällen der Anwendungsanbieter (5 Projekte) und außerdem werden Public-Cloud-Lösungen (5 Projekte) gewählt.

Die meisten gewählten LLMs sind zumindest in Teilen Open Source, das bedeutet, mindestens die Gewichte sind Open Source. Auf unterschiedliche Versionen von LlaMA (11) fiel am häufigsten die Entscheidung. Meta hat die Gewichte der LlaMA-Modelle als Open Source veröffentlicht, hält aber wichtige Informationen wie die Trainingsdaten unter Verschluss und erfüllt somit nur teilweise die Anforderungen an Open Source, wie in Abschnitt 3.2 beschrieben. An zweiter Stelle landet als europäische Alternative Mistral (7), für die ebenfalls Informationen zum Trainingsprozess nicht veröffentlicht werden. Auch DeepSeek (3) wurde angegeben. Als einzige Nicht-Open-Source-Option wurden Modelle von OpenAI (5) verwendet. Im Sinne der *Wechselmöglichkeit* wurde danach gefragt, ob sich innerhalb der Anwendung flexibel zwischen LLMs verschiedener Anbieter wechseln lässt. Das ist der Fall bei einem Drittel der Projekte (11) und einem weiteren Projekt, bei dem sich nur zwischen LLMs eines einzelnen Anbieters wechseln lässt. Das spiegelt sich auch in den gewählten Preismodellen für die LLMs wider: Aufgrund der großen Bedeutung des Eigenbetriebes von Open-Source-Produkten gab nur ein kleiner Teil der Projekte (4) an, auf ein bestehendes Preismodell zurückzugreifen, während alle anderen kein kostenpflichtiges Modell nutzen (19) respektive keine Angabe (10) machten. Kein Projekt gab an, dass die Server außerhalb der EU stehen.

Eine interessante Beobachtung ist, dass fast ausschließlich öffentliche (13) und eigene Daten (13) verwendet werden. Zu den eigenen Daten wurden unter anderem Forschungsdaten, Antragsdaten und semi-öffentliche Daten eines Wiki-Systems für Mitarbeitende genannt. Kommerzielle Daten wurden nur in geringer Anzahl genutzt (4). Hier wurden ebenfalls Forschungsdaten genannt. Das zeigt, dass hoher Bedarf daran besteht, eigene Daten mithilfe von LLMs zugänglicher und handhabbarer zu machen. Aus den Interviews ergab sich, dass dafür eine ausreichend gute Datenqualität als eines der großen Hindernisse in der Entwicklung gesehen wird. So erschweren in manchen Projekten das Fehlen eines einheitlichen Dokumentenmanagementsystems und die Heterogenität der Daten (Bilder, Scans als PDF, Videos, Texte, Konstruktionszeichnungen in unterschiedlichen Formaten) die Weiterverarbeitung zum Beispiel in

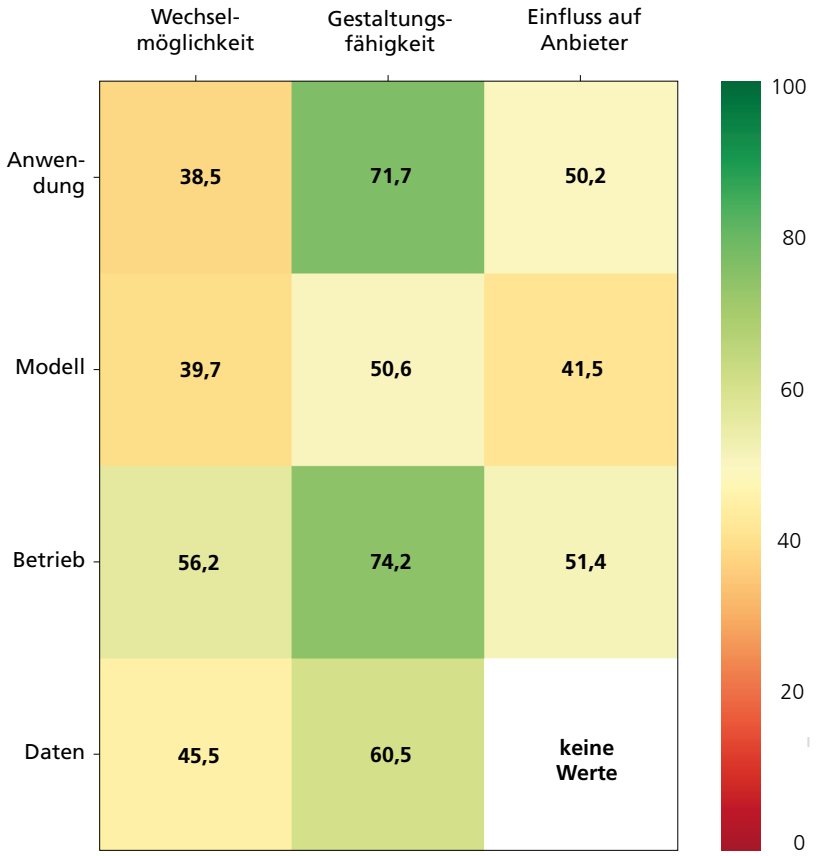


Abbildung 7: Heatmap möglicher Schmerzpunkte aus der Auswertung der Indikatormatrix über alle betrachteten Projekte

Vektordatenbanken. Obwohl es inzwischen in vielen Häusern eigene Datenlabore gibt, bleiben also Hürden bestehen. Das ist unter anderem dadurch erklärbar, dass die Qualität bestehender Daten häufig nicht oder nur mit unverhältnismäßigem Aufwand nachträglich verbessert werden kann. Es ist also davon auszugehen, dass zukünftig Daten in höherer Qualität vorliegen werden, bestehende Daten jedoch teilweise weiterhin nicht nutzbar sind.

6.3.3 Indikatormatrix

Auf Basis der Erhebung und des Indikatorkataloges (siehe Anhang A.5) wurden Scores für die Souveränitätsziele berechnet (siehe Abbildung 7). Der Wert jedes Matrixeintrages ist der Durchschnitt über die Ausprägung einer Reihe von Indikatoren pro Projekt. Das heißt, für jeden Matrixeintrag gibt es mehrere Indikatoren, die (wie in Abschnitt 2 beschrieben) Ausprägungsstufen von 0–3 annehmen können. Die maximale Punktzahl pro Matrixeintrag ist 100. Insgesamt zeichnet die Matrix ein gutes Bild mit hohen bis mittleren Werten in allen 12 Feldern. Die Ergebnisse finden sich aufgeschlüsselt nach Indikatoren im Anhang A.6.

Die höchsten Werte (76,2 respektive 74,2) wurden beim Ziel *Gestaltungsfähigkeit* auf den Ebenen Anwendung und Betrieb erzielt. Das überrascht wenig, handelt es sich bei den meisten Projekten um In-House-Entwicklungen: Zugehörige Indikatoren sind unter anderem die technische und fachliche Kompetenz, die, wie bereits beschrieben, als gut bis sehr gut eingeschätzt wird. Die weiteren Indikatoren in diesem Feld (Zusammenarbeitsstrukturen und Anwendungsdokumentation) erzielten im Durschnitt ebenfalls (wie beschrieben) gute Werte. Mittlere Werte (50,6 und 60,5) wurden beim Ziel der *Gestaltungsfähigkeit* bei Modell und Daten erzielt. Auf Ebene des Modells wurde geschaut, wie gut die Informationsbereitstellung der LLM-Anbieter eingeschätzt wird, da dies Einfluss auf die eigenständige Nutzung haben kann. Ebenfalls flossen die Indikatoren Open Source, KI-spezifische Kompetenz und Zusammenarbeitsstrukturen in diesen Wert ein. Auf Ebene der Daten wurde erhoben, wie einfach es möglich ist, Daten nach Bedarf auszutauschen. Außerdem wurde nach der Quelle der Daten gefragt und dabei zwischen eigenen Daten, öffentlichen Daten und kommerziellen Daten unterschieden. Das insgesamt gute Abschneiden im Bereich der *Gestaltungsfähigkeit* (65,4) zeigt ein gewisses Selbstvertrauen der Projektverantwortlichen in die eigenen Kompetenzen im Team sowie funktionierende (auch behördenübergreifende) Zusammenarbeitsstrukturen. Aus Souveränitätsperspektive besteht hier daher aktuell kein großer Handlungsbedarf. Im Gegenteil kann aus dieser Einschätzung geschlossen werden, dass sich die Bundesverwaltung durchaus in der Lage sieht, anbieterunabhängig selbstständig LLM-Systeme zu entwickeln.

Gute bis mittlere Werte wurden beim Ziel der *Wechselmöglichkeit* auf Ebene des Betriebes erzielt (56,2). Dieser Wert ergibt sich aus der Tatsache, dass viele der Projekte auf Eigenbetrieb setzen: Dabei wird davon ausgegangen, dass dies einen Wechsel prinzipiell erleichtert. Nicht berücksichtigt wird jedoch der technische und finanzielle Aufwand, den ein Wechsel möglicherweise, je nach den individuellen Voraussetzungen, ergeben kann. Aus Perspektive der Souveränität ist es daher wichtig, zu schauen, inwieweit die Hardware für den Eigenbetrieb konsolidiert werden sollte und so einerseits (mehr) Möglichkeiten einer gemeinsamen Nutzung geschaffen werden und andererseits die Notwendigkeit KI-spezifischer Hardwarebeschaffungen einzelner Häuser den Verantwortlichen nicht mehr notwendig erscheinen.

Ebenfalls mittlere Werte wurden beim Ziel *Einfluss auf Anbieter* bei Anwendung (50,2) und Betrieb (51,4) erzielt. Das Ziel *Einfluss auf Anbieter* muss im Kontext dieser Studie als etwas weniger wichtig eingeordnet werden, da es sich bei den Projekten zu einem großen Teil um Eigenentwicklungen handelt, die nicht im eigentlichen Sinne in einem Verhältnis zu einem Anbieter stehen. Drei Indikatoren zahlen auf die Ebene der Anwendung ein: Zertifikate, Ökosystem und rechtliche Kompetenz. Bei Zertifikaten wurde erfragt, ob es vom Anwendungsanbieter Garantien bezüglich digitaler Souveränität gibt. Das war nur relevant bei Projekten, die den Entwicklungsprozess ausgelagert haben. Bei diesen gab es teilweise vertragliche Garantien, dass die Entwicklung Eigentum der Behörde ist. Aus den Daten lässt sich daher insgesamt nur bedingt abschätzen, wie es um den *Einfluss auf Anbieter* im Bereich LLMs steht. Für eine bessere Bewertung bräuchte es eine größere Datenbasis von Projekten, die Beschaffungsmaßnahmen vorgenommen und Verträge mit Anbietern abgeschlossen haben.

Mit den genannten Einschränkungen ergibt sich aus der Indikatormatrix in den meisten Bereichen also ein im Durchschnitt gutes Bild, insbesondere die dem Ziel der *Gestaltungsfähigkeit*. Das ist jedoch nicht das ganze Bild: Im nächsten Abschnitt werden die Hürden und sich möglicherweise ergebenden Schmerzpunkte thematisiert, die sich in der Indikatormatrix durch geringere Punktzahlen in einzelnen Feldern andeuten.

6.4 Hürden und Schmerzpunkte

Die *Wechselmöglichkeit* auf Ebene der Anwendung (38,5) und des Modells (39,7) ist eher gering, obwohl über fast alle Projekte hinweg angegeben wurde, die Anwendung sei modular oder sehr modular aufgebaut (eine Voraussetzung für den Wechsel von Komponenten). Die eher geringen Werte ergeben sich aus einem anderen Indikator: Zwar wird für die LLMs vorrangig auf Open-Source-Modelle zurückgegriffen, aber es plant oder stellt nur ein knappes Drittel (11) der öffentlichen Betreiber ihre Anwendung selbst als Open Source zur Verfügung, macht sie

nachnutzbar und erhöht so die Anzahl an (erprobten) Alternativen für die Verwaltung. Das hat Auswirkungen auf das Ziel der *Wechselmöglichkeit*, das grundsätzlich von der Verfügbarkeit alternativer Lösungen profitiert. In einigen Fällen wurde die Entscheidung gegen Open Source mit einem als unklar oder unverhältnismäßig empfundenen (rechtlichen) Aufwand beispielsweise bei der Wahl der angemessenen Lizenzen begründet. Hier zeigt sich auch, dass die teilweise als gering eingestuften rechtlichen Kompetenzen eine Hürde hin zu mehr Open Source bedeuten können.

Die Wechselfähigkeit auf der Ebene der Daten wurde als ein möglicher Schmerzpunkt identifiziert, der auch in den Interviews mehrfach genannt wurde. Dabei geht es weniger um Lock-in-Effekte bei der Nutzung kommerzieller Daten, sondern um grundlegende Herausforderungen für die Nutzung der eigenen Daten. Genannt wurde etwa, dass die hohe Datenheterogenität die Nutzbarmachung erschwert, der Datenaustausch zwischen Behörden weiterhin schwierig und die Erfüllung der rechtlichen Voraussetzungen für (vertrauliche) Datennutzung herausfordernd sei. Unklar ist geblieben, inwieweit die Datenlabore der Behörden hier mittelfristig Abhilfe schaffen können. Eine Schwierigkeit besteht darin, dass die Qualität bestehender Daten oft nicht oder nur mit unverhältnismäßigem Aufwand nachträglich verbessert werden kann.

Ein geringerer Wert wurde außerdem bei *Einfluss auf Anbieter* auf Ebene des Modells erzielt. Auch hier könnten die vergleichsweise geringen rechtlichen Kompetenzen innerhalb der Projektteams in einem Umfeld sich rasch ändernder und mitunter unklarer rechtlicher Lage zu KI ein Risiko bergen. Das führte teilweise dazu, dass Projekte größere Einschnitte in Funktionalität oder Verfügbarkeit hinnahmen. Statt höherer rechtlicher Kompetenzen werden einfachere und klarere Rahmenbedingungen gewünscht.

Trotz eines mittleren Wertes der Wechselfähigkeit auf Ebene des Betriebes stellte sich ein Schmerzpunkt durch die Interviews heraus: Das betrifft die Verfügbarkeit von KI-spezifischer (Cloud-)Infrastruktur. Es wurde der Wunsch geäußert, auf geteilter Hardware für alle Häuser Open-Source-Sprachmodelle zur gemeinsamen Nutzung zu hosten. Häuserspezifische Software könnte weiterhin in-house entwickelt werden, allerdings fiele die Notwendigkeit weg, eigene KI-spezifische Hardware für die LLMs zu betreiben.

Insgesamt zeigen sich somit auch Herausforderungen in den Projekten, was potenziell negative Auswirkungen auf die drei Souveränitätsziele haben kann.

Im nächsten Abschnitt werden alle Erkenntnisse dieses und der vorigen Abschnitte zusammengeführt.

7. Kernergebnisse

Ziel der Studie war es, eine fundierte Einschätzung zu geben, wie die digitale Souveränität der Bundesverwaltung durch die Entwicklungen zu LLMs beeinflusst wird. Unter diesem Gesichtspunkt wurde eine Marktbetrachtung durchgeführt, es wurden bestehende Maßnahmen zur Stärkung digitaler Souveränität diskutiert, es wurde ein vergleichender Blick in das (europäische) Ausland geworfen und es wurde – als Hauptteil der Studie – eine Datenerhebung und -analyse von LLM-Entwicklungen der Bundesverwaltung durchgeführt. Aus diesen Quellen ergibt sich ein Lagebild, das – trotz eines recht konzentrierten Marktgeschehens und der Marktmacht einiger weniger Unternehmen vor allem im Bereich der Hardware – insgesamt positiv ist. **Aus unserer Sicht können die derzeitigen (Eigen-)Entwicklungen von LLM-Lösungen dazu beitragen, dass durch die Einführung der Technologie keine neuen Abhängigkeiten entstehen oder bestehende vertieft werden.** Anders als unter anderem die Studie zur Bürosoftware der Bundesverwaltung, die starke Abhängigkeiten zu einem einzelnen Anbieter feststellte (PwC 2019), lässt sich im Bereich der LLMs keine solche singuläre Beziehung feststellen.

Die Ergebnisse zeigen im Besonderen, dass bei der (Eigen-) Entwicklung von verwaltungsinternen LLM-Systemen bereits einiges im Sinne der Wahrung der digitalen Souveränität getan wird. In den Interviews mit den Projektverantwortlichen offenbarte sich eine Sensibilität für die Wahrung digitaler Souveränität, die Berücksichtigung bei der Projektentwicklung fand, zum Beispiel im Betrieb geeigneter Open Source LLMs auf eigener Hardware. Dass die wenigsten Modelle als vollständig Open Source nach dem Verständnis aus Abschnitt 3.2 gelten, sehen wir aus Perspektive der Betriebs- und Entwicklungssouveränität als wenig kritisch: Solange das Modell durch vertrauenswürdige Anbieter oder eigenständig betrieben werden kann, droht kein Lock-in. Es ist aber zu beobachten, dass sich auf Basis entsprechender funktionaler bzw. qualitativer Gesichtspunkte vorrangig für OSS-Lösungen nichteuropäischer Anbieter entschieden wurde.

Von besonderer Relevanz sind behördenübergreifende Systeme, aufgrund ihrer Reichweite und dem potenziellen Einfluss auf die Verwaltungshandlungsfähigkeit. Dazu zählen solche, welche die typischen LLM-Anwendungspotenziale wie Textzusammenfassungen, Übersetzungen oder auch RAG-basiertes Arbeiten anbieten. Einen besonderen Mehrwert generieren diese Lösungen in dem Moment, wo verwaltungsinterne Daten – unter Umständen sogar als VS-NfD eingestufte – durch diese Systeme verarbeitet werden dürfen. Dies stellt die Entwickler:innen vor besondere Herausforderungen bezüglich der Informationssicherheit, weswegen zum Zeitpunkt der Studie noch keines der untersuchten Systeme diese Anforderung erfüllte, mindestens zwei jedoch laut eigener Aussage kurz davorstehen.

Gleichzeitig ist darauf hinzuweisen, dass eine Reihe an Fragen durch diese Studie unbeantwortet bleiben (müssen). Insbesondere könnte es sinnvoll sein, in einer möglichen Folgestudie einen stärker nutzer:innen-zentrierten Blick einzunehmen. Außerdem fällt auf, dass die starke Einbettung von LLMs in bestehende Umgebungen eine »getrennte« Betrachtung erschwert. Folgestudien könnten hier einen noch stärker integrativen Ansatz wählen.

Weitere Anknüpfungspunkte finden sich in einer Auseinandersetzung mit (gemeinsamen) Cloudlösungen. Hier ist insbesondere die deutsche Verwaltungscloud (DVC) zu nennen. Inwieweit diese die Voraussetzungen mit sich bringt, auch für (hardware-) technisch sehr anspruchsvolle KI-Lösungen genutzt werden zu können, bleibt offen. In einigen Interviews wurde eine gemeinsame, verwaltungsübergreifende, rechtssichere Cloud-Infrastruktur gewünscht, welche hardware- und softwaretechnisch dafür besser ausgestattet ist und personell kompetent betreut wird, um KI-Anwendungen, die von Häusern oder externen Anbietern entwickelt wurden, zentral bereitzustellen.

Schließlich könnte eine gesonderte Betrachtung und Bewertung der größten Eigenentwicklungen mit Fokus auf digitaler Souveränität sinnvoll sein. Das meint: Eine Bestimmung, inwieweit das Produkt/die Dienstleistung (perspektivisch) auch für das Erreichen kritischer staatlicher Ziele eingesetzt werden wird und damit besondere Anforderungen an die Garantie eines Betriebes ohne Schmerzpunkte gelten. Je höher diese sogenannte

strategische Relevanz, desto höher der Souveränitätsbedarf. Eine solche Analyse konnte aufgrund der Breite dieser Studie nicht durchgeführt werden und könnte unter anderem betrachten, inwieweit ein System (a) bei einem Wegfall (negative) Auswirkungen für Bürger:innen hervorruft, (b) hohe oder höhere Bedeutung für äußere Sicherheit hat, (c) weitreichende Zugriffe auf Verwaltungsinformationen bzw. Geheimhaltungspflichten hat oder (d) ggf. als Hochrisikosystem im Rahmen der KI-Verordnung gesehen wird.

Es sollte nicht vergessen werden, dass es auch auf Ebene der (Bundes-)Länder Entwicklungen zur Nutzung von LLMs gibt. Möglicherweise könnten hier Kräfte gebündelt werden, um statt mehrerer »gleicher« Lösungen, die parallel laufen, eine gemeinsame Plattform zu schaffen. Auch hier könnte es sinnvoll sein, eine Studie anzustoßen, die über die föderalen Ebenen hinweg LLM-Projekte in den Blick nimmt.

Es ist davon auszugehen, dass die Weiterentwicklung der Technologie mit hoher Geschwindigkeit vorangeht. Dabei sollten sich abzeichnende Trends besonders im Auge behalten werden. Dazu gehören kleinere Sprachmodelle als Alternative für spezifische Anwendungsfälle. Nicht immer werden die größten und rechenintensivsten Modelle benötigt. Stattdessen ist es hilfreich, ausgehend von dem zu lösenden Problem die geeignete Architektur zu wählen. Unter Umständen kann es sinnvoll sein, kleinere Sprachmodelle zu verwenden, die im Umkehrschluss leichter zu trainieren sind und weniger Ressourcen kosten. Auch die weitere Entwicklung im Bereich der KI-Agenten sollte beobachtet werden. Wie in Abschnitt 1.2 skizziert, ist das Potenzial dieser Technologie für die Verwaltung groß. Schließlich ist davon auszugehen, dass in der nahen Zukunft neue, leistungsstärkere Sprachmodelle auf den Markt kommen, möglicherweise auf Basis neuer Architekturen und/oder Trainingsmethoden, entwickelt von den im Abschnitt 3.1 thematisierten Technologieunternehmen.

8. Handlungsempfehlungen

Was kann getan werden, um die derzeit vielversprechenden Ansätze innerhalb der Verwaltung zu stärken und mittel- bis langfristig nicht in neue Abhängigkeiten durch LLM-Technologie zu geraten? Die Gefahr ist real, dass, falls die Anwendungen der großen Technologiekonzerne (mangels gleichwertiger Alternativen) in der Breite eingesetzt werden (müssen), sich ähnliche Abhängigkeitsverhältnisse herausbilden, wie es bei anderen Softwarelösungen derzeit der Fall ist (vgl. PwC 2019). Das könnte passieren, wenn die Eigenentwicklungen, die auf Open-Source-Lösungen setzen, aus unterschiedlichen Gründen nicht in der Breite angenommen oder aber relativ kurzfristig nicht über föderale Grenzen hinweg verfügbar gemacht werden. Außerdem weist die relative Schwäche der einbezogenen Projekte auf der Betrachtungsebene der LLMs darauf hin, dass hier mehr getan werden sollte. Im Folgenden werden zukunftsgerichtete Handlungsempfehlungen organisatorischer, rechtlicher, technischer und strategischer Natur in vier thematischen Clustern vorgestellt, die sich teilweise aus den Erkenntnissen dieser Studie ergaben und sich auch aus der Diskussion mit Expert:innen speisen, also über den Kern der Studie hinaus reichen. Sie sind so strukturiert, dass jeweils ein Ziel formuliert ist, ein grobes Vorgehen skizziert wird sowie Zeithorizont, Vorteile und Risiken eingeschätzt werden.

8.1 Gemeinsame Infrastruktur

8.1.1 Gemeinsame Nutzung von KI-Hardware-Ressourcen anstreben

Dimension: Technisch-organisatorisch
Zeithorizont: Mittelfristig
Ziel: GPU-Ressourcen in abgestuft gesicherten Bereichen zentral aufbauen beziehungsweise zusammenführen

Einordnung: Der Betrieb generativer KI-Anwendungen erfordert spezialisierte Hardware-Ressourcen, insbesondere GPUs. Derzeit sind diese Ressourcen in der Bundesverwaltung mitunter an einzelnen, sehr spezifischen Stellen vorhanden, etwa als Einzelanschaffungen in Fachbehörden. Jedoch findet auch oft nur rudimentär geregeltes Ausprobieren auf den Webplattformen großer, weitgehend US-amerikanischer Anbieter statt. Eine koordinierte, zentralisierte Bereitstellung innerhalb abgestuft gesicherter IT-Schutzzonen ggf. zusammen mit Teilnehmenden aus der deutschen Wirtschaft würde nicht nur die Effizienz erhöhen, sondern auch die Kontrolle über diese potenziell kritische Infrastruktur stärken. Ziel sollte es daher sein, gemeinsam nutzbare GPU-Kapazitäten aufzubauen und auch für die Länder und Kommunen (z. B. über die Deutsche Verwaltungscloud) verfügbar zu machen.

Vorgehensweise: Ressourcenbündelung im Bund: Bestehende GPU-Ressourcen im Bund sollten zentral inventarisiert und – wo technisch möglich – zusammengeführt werden. Die Neuanschaffung sollte koordiniert erfolgen, um Parallelstrukturen zu vermeiden und einen größeren Hebel gegenüber den Anbietern zu haben (*Einfluss auf Anbieter*). Die Bündelung muss mit den bestehenden Sicherheits- und Datenschutzanforderungen vereinbar sein. Lock-in-Effekte sollten vermieden werden. Die Ressourcen sollten je nach Schutzbedarf von Daten und Anwendungen in entsprechend geeigneten Schutzzonen bereitgestellt werden. Die Länder sollten dabei von Anfang an mitgedacht werden, da auch auf Länderebene bereits einige LLM-Lösungen entwickelt und betrieben werden. Dies kann etwa im Rahmen föderaler Plattformmodelle (vgl. 9.1.1) oder gemeinsamer Rechenzentrumsstrukturen geschehen. Dafür braucht es klare Betriebs- und Nutzungsmodelle sowie standardisierte Schnittstellen, damit verschiedene Organisationseinheiten verlässlich darauf zugreifen können. Eine zielgerichtete Zusammenarbeit mit Teilnehmenden aus der Wirtschaft, wie im Koalitionsvertrag festgelegt, kann zur Stärkung des Wirtschaftsstandorts beitragen.

Vorteile:

Die Zusammenlegung und der gemeinsame Betrieb von leistungsfähiger KI-Hardware führen zu verschiedenen Vorteilen.

– Leistungsfähige, zentralisierte KI-Rechenzentren ermöglichen die gemeinschaftliche, effizientere Nutzung von LLMs und anderen KI-Modellen.

- Durch die gemeinsame Nutzung der Hardware wird eine höhere Auslastung und bessere Wirtschaftlichkeit der vorhandenen Ressourcen erreicht.
- Die bessere Wirtschaftlichkeit kann die Anschaffung von leistungsfähiger Spezialhardware oder besonderer Funktionalitäten (z. B. ausfallsichere Georedundanz) rechtfertigen/ermöglichen.
- Mit Bündelung der Hardware und kann auch die fachlich-technische Kompetenz gebündelt werden.
- In Zusammenarbeit mit der Wirtschaft können hochqualifizierten Fachkräften attraktive Konditionen gezahlt werden. Dem Fachkräftemangel der öV kann so begegnet werden.

Risiken:

Das Vorhaben der Bereitstellung einer zentralen KI-Infrastruktur ist mit verschiedenen Risiken und Unsicherheiten verknüpft.

- Es ist unklar, wie und unter welchen Bedingungen bestehende KI-Hardware aus dem Bund und den Ländern zusammengeführt werden könnte.
- Es besteht die Gefahr, dass schon bestehende KI-Hardware eine technische Inkompatibilität aufweist und nicht gemeinsam betrieben werden kann.
- Das Zusammenführen von KI-Hardware kann auf Widerstände von bzw. Ablehnung durch einzelne Institutionen führen.
- Für den gemeinsamen Betrieb von KI-Hardware sind verschiedene organisatorische und rechtliche Voraussetzungen zu schaffen, die einen unklaren zeitlichen Horizont haben.
- Die Nutzung der Infrastruktur durch Kundenbehörden erscheint evtl. im Vergleich zu Marktangeboten großer Hyperscaler als zu teuer.

Empfehlung: Die Bundesregierung sollte eine sichere und leistungsfähige KI-Cloud-Infrastruktur zentral bereitstellen. Ein geeigneter IT-Dienstleister der öV oder ein privater, deutscher Wirtschaftsanbieter könnte beauftragt werden, zentrale GPU-Ressourcen für GenKI-Anwendungen aufzubauen und zu betreiben. Für die Zusammenführung bei einem IT-Dienstleister der öV wären Fördermodelle denkbar, um bestehende Einzelbeschaffungen schrittweise zu migrieren. Die Infrastruktur sollte so ausgelegt werden, dass Länder, öffentliche Einrichtungen und evtl. auch private Wirtschaftsteilnehmer darauf zugreifen können.

8.1.2 GenKI-Lösungen föderal bündeln und bereitstellen

Dimension: Organisatorisch, technisch
Zeithorizont: Mittelfristig
Ziel: Aufbau einer gemeinsamen, föderal übergreifenden GenKI-Lösung für die öffentliche Verwaltung

Einordnung: Derzeit laufen in mehreren Behörden und auf verschiedenen föderalen Ebenen Projekte zum Einsatz generativer KI, meist noch ohne übergreifende Koordination. Dies kann zu Insellösungen, redundanten Entwicklungen und erhöhtem Abstimmungsbedarf führen. Eine föderal nutzbare GenKI-Lösung würde ermöglichen, häufige Anwendungsfälle – etwa in der Texterstellung, bei Assistenzsystemen oder der Dokumentenanalyse – standardisiert, interoperabel und rechtssicher anzubieten. Dabei sollte eine solche Lösung modellagnostisch sein, sodass die Nutzenden frei in der Wahl der LLMs sind. Klar definierte, offene Schnittstellen ermöglichen die Entwicklung von Lösungen durch Teilnehmende der privaten Wirtschaft, welche der Staat als Ankerkunde einsetzen kann.

Vorgehensweise: Ausgehend von einem gemeinsamen Zielbild, das sich am geplanten Deutschland-Stack und an bestehenden digitalen Infrastrukturen orientiert, sollte eine Referenzarchitektur gemeinsam durch Bedarfsträger und Fachexpertinnen und -experten entwickelt werden. Eine modulare Architektur stellt sicher, dass unterschiedliche Anforderungen integriert und einzelne Module ausgetauscht werden können. Es sollte die Interoperabilität der bestehenden Systeme analysiert werden. GenKI-Lösungen in Bund und Ländern können auf Anschlussfähigkeit geprüft werden, um idealerweise eine Konvergenz der verschiedenen Lösungen für einen generischen Anwendungsfall hin zu einer (oder wenigen) gemeinsamen Lösung(en) zu ermöglichen. Durch Beteiligung und Einbindung von Partnern aus der privaten Wirtschaft, werden Anreize geschaffen, um innovative Lösungen für die Verwaltung zu entwickeln. Wo möglich, sollte eine Zusammenführung bestehender Systeme angestrebt werden (z. B. innerhalb der DVC).

Vorteile:

- Durch die Bereitstellung einer gemeinsamen GenKI-Anwendung wird die Anzahl redundanter Entwicklungen reduziert und die Nachnutzbarkeit einzelner Lösungen erhöht. Da die einzelnen Lösungen von mehr Institutionen genutzt werden, sinkt der Ressourcenverbrauch pro Institution (Skaleneffekte treten auf).
- Mit der Bündelung der Kompetenzen und Fachexpertisen wird zur Schaffung eines einheitlichen, vertrauenswürdigen Angebotes für GenKI-Anwendungen beigetragen.

Risiken:

- Sofern bestehende Lösungen nicht nachnutzbar sind, ist zu erwarten, dass diese Lösungen weiterhin durch die Bestandskunden genutzt werden. Skaleneffekte, die durch nachnutzbare Lösungen auftreten, fallen so kleiner aus.

Empfehlung: Die Bundesregierung sollte in Abstimmung mit den Ländern im IT-Planungsrat ein Projekt zur Erarbeitung einer gemeinsamen GenKI-Plattform aufsetzen. Beim Projekt sollte

die Einbindung bestehender Entwicklungen berücksichtigt und insbesondere geschaut werden, ob und, wenn ja, wie diese zusammengeführt werden können. Durch Beteiligung von Teilnehmenden aus der privaten Wirtschaft können die Rahmenbedingungen für eine spätere Einbindung von Angeboten deutscher oder europäischer Firmen definiert werden.

8.1.3 Unterstützungsangebote zur Einführung generativer KI schaffen und institutionell verankern

Dimension: Strategisch, organisatorisch
Zeithorizont: Kurzfristig
Ziel: Integriertes Angebot zur Einführung generativer KI, das über die rein technische Dimension hinausgeht und bei der Einführung begleitet, Kompetenz aufbaut und (rechtliche) Beratung einschließt

Einordnung: Die Einführung generativer KI in der Bundesverwaltung ist nicht allein eine technische Frage. Behörden benötigen Orientierung, praktische Begleitung sowie Hilfe bei rechtlichen, ethischen und organisatorischen Fragestellungen. Einzelne technische Lösungen sind ohne flankierende Unterstützungsangebote und dem richtigen Kompetenzaufbau oft nicht wirksam nutzbar. Ziel ist daher die Entwicklung integrierter Unterstützungsangebote (vergleichbar mit den DVC-Lotsen), die Einführungsberatung, Schulungen, Musterprozesse, rechtliche Einschätzungen und Governance-Modelle in einem Paket umfassen. Damit wird GenKI für möglichst viele Stellen sinnvoll nutzbar gemacht – ohne sich alle KI-Kompetenz von Grund auf allein aneignen zu müssen (Wachsmann und Weber 2025).

Vorgehensweise: Die Umsetzung sollte über eine Stärkung und strategische Weiterentwicklung des Beratungszentrums für Künstliche Intelligenz (BeKI) erfolgen. Das BeKI kann die zentrale Anlaufstelle für Behörden werden, die generative KI einführen möchten, und sollte hierzu personell und fachlich ausgebaut werden (KI-Lotsen). Gleichzeitig ist eine enge Verzahnung mit bestehenden und entstehenden technischen Plattformangeboten sicherzustellen – etwa durch Kooperationsvereinbarungen auf Bundes- und Länderebene. Die Unterstützungsleistungen sollten modular aufgebaut sein, sodass sie je nach Reifegrad der Behörde angepasst werden können – von niedrigschwelliger Erstberatung über gezielte Schulungsangebote bis hin zu juristischer Begleitung in komplexeren Szenarien. Zur inhaltlichen Tiefe und Breite des Angebotes sollte das BeKI auch mit bestehenden KI-Kompetenzzentren (z. B. des BMFTR), rechtlichen Fachstellen und themenspezifischen Referaten zusammenarbeiten, um ein qualitativ hochwertiges und vertrauenswürdiges Gesamtpaket anbieten zu können.

Vorteile:

- Die KI-Lotsen erleichtern den Einstieg in den Einsatz generativer KI insbesondere für kleinere oder KI-fachfremde Behörden.
- Durch die geplanten Unterstützungsleistungen wird die flächendeckende, qualifizierte Einführung von GenKI beschleunigt.
- Als klare Anlaufstelle für rechtliche und ethische Fragestellungen wird Unsicherheiten bei Pilotierungen vorgebeugt und Lösungen können früher in den produktiven Einsatz gehen.
- Durch eine frühe, abgestimmte Beratung, die einen Überblick über das Gesamtangebot hat, kann Fehlentwicklungen und unnötigen Redundanzen vorgebeugt werden.

Risiken:

- Es besteht ein hoher Bedarf an qualifiziertem Personal mit KI- und Verwaltungs-Know-how, der nur schwierig gedeckt werden kann.
- Für den Aufbau und die Verstetigung der Unterstützungsstruktur sind zusätzliche Stellen und Kosten einzuplanen. Die (Re-)Finanzierung kann sich herausfordernd gestalten.

Empfehlung: Die Bundesregierung sollte kurzfristig die institutionelle und finanzielle Stärkung des BeKI prüfen und dieses mit einer aktiven Koordinierungsrolle für integrierte GenKI-Angebote betrauen. Dazu gehört die enge Verzahnung mit bestehenden technischen Plattformen und Infrastruktur. Ein standardisiertes Unterstützungsportfolio könnte entwickelt werden, das bundesweit abrufbar ist – etwa in Form eines modularen »GenKI-Startpakets« für Behörden.

8.2 Open Source

8.2.1 Europäisches, offenes (Verwaltungs-)LLM entwickeln

Dimension: Strategisch, technisch
Zeithorizont: Kurz- bis mittelfristig
Ziele: Durch die Entwicklung und Bereitstellung eines vollständig offenen LLMs soll erreicht werden: Längerfristige Unabhängigkeit von marktbeherrschenden LLM-Anbietern; Berücksichtigung europäischer Werte und spezifischer Verwaltungsbedarfe; Innovationsförderung für das KI-Ökosystem

Einordnung: Die Analyse der KI-Projekte der Bundesverwaltung hat gezeigt, dass im Bereich der LLMs relative Schwächen hinsichtlich der digitalen Souveränität bestehen, die trotz konkreter Adressierung der Herausforderungen in den Projekten – etwa durch die Verwendung von Open-Source-Modellen – nicht vollständig ausgeglichen werden können. Zugleich verschwimmen die Grenzen zwischen Open Source und proprietären Modellen

etwa durch die nur noch punktuelle Erfüllung der Kriterien für freie und offene Software, während die geopolitischen Entwicklungen eher auf weniger vertrauensvolle Zusammenarbeit über Staatgrenzen hinweg hindeuten. Vor diesem Hintergrund und zur Sicherstellung der Berücksichtigung von verwaltungsspezifischen Anforderungen könnte die Entwicklung eines eigenen, auf europäische Normen und Werten ausgerichteten LLMs sinnvoll sein – etwa im Hinblick auf Datenschutz, Sprache, Barrierefreiheit, Sicherheit oder Nachvollziehbarkeit. Ein solches LLM könnte gemeinsam mit europäischen Partnern aufgebaut und betrieben werden und im Rahmen von weitreichenden Open-Source-Standards bereitgestellt werden. Die Entwicklung würde keine kommerziellen Ziele verfolgen, sondern auf Vertrauenswürdigkeit, Verantwortlichkeit und öffentliche Zugänglichkeit ausgerichtet sein. Zugleich muss das neu entwickelte LLM bei Erscheinen praktische Mehrwerte gegenüber bestehenden, hoch performanten Modellen bieten. Angesichts der Geschwindigkeit der technologischen Entwicklung würde anderenfalls riskiert, dass die finanziellen und ökologischen Kosten für die Entwicklung und das Training eines eigenen Modells unnütz aufgewendet werden. Ein eigenes LLM muss selbst ein Innovationstreiber sein, auch um die auf der Entwicklung aufbauenden, datengetriebenen Geschäftsmodelle auch für europäische Unternehmen zu ermöglichen. Auch dies stärkt die digitale Souveränität des Wirtschaftsstandortes. Entsprechend ist das LLM nicht der Endpunkt der Entwicklung, sondern der Startpunkt für eine weitergehende, europäisch geprägte Innovationsdynamik.

Vorgehensweise: Ausgangspunkt bildet eine Bestandsaufnahme und Analyse der bereits vorhandenen deutschen und europäischen LLMs und der darauf zielenden Initiativen. Darauf aufbauend lassen sich sowohl relevante Akteure als auch technologische Herausforderungen identifizieren und erwartbare Aufwände ermitteln. Die Entwicklung des LLMs selbst muss sich dann an den FOSS-Prinzipien ebenso orientieren wie an Anforderungen zu Datenschutz, IT-Sicherheit, ethischen Standards, öffentlichen Bedarfen und der Minimierung ökologischer Kosten. Ziel ist es nicht nur, mit vorhandenen LLMs hinsichtlich Performanz und Wirtschaftlichkeit gleichzuziehen, sondern diese bei den weitergehenden Kriterien zu übertreffen. Begleitend dazu ist die Schaffung eines europäischer Trainingsdatenraums erforderlich.

Vorteile:

- Eine adäquate leistungsfähige Alternative zu außereuropäischen LLM-Anbietern führt langfristig zu einer hohen digitalen Souveränität in diesem Bereich.
- Die Eigenentwicklung ermöglicht eine vollständige Kontrolle über den gesamten Prozess. Mit einer Einbindung von Wissenschaft und Wirtschaft wird angestrebt, das LLM nicht nur technisch gleichwertig oder besser als existierende Lösungen, sondern auch nach ethischen Maßstäben und europäischen Werten zu gestalten.
- Die Bereitstellung eines solchen LLMs garantiert eine längerfristige Unabhängigkeit von Marktverhältnissen und proprietären Geschäftsmodellen.
- Eine transparente Wahl der Trainingsdaten und ein transparenter Trainingsprozess, bei dem europäische Werte wie Datenschutz, Teilhabe und Nachhaltigkeit berücksichtigt werden (bei gleichzeitiger hoher Performanz), kann als Alleinstellungsmerkmal weltweit Aufmerksamkeit generieren.
- Die europäische Wirtschaft und Verwaltung profitiert von einem solchen LLM. Es könnte die Erschließung neuer Geschäftsmodelle erleichtern und Innovationspfade erschließen, da ein LLM mit »europäischem Gütesiegel« Hemmnisse und Bedenken in der Nutzung auch für kleinere Einheiten (KMUs, kommunale Verwaltung) abbaut.

Risiken:

- Ein solches Projekt ist mit sehr hohen einmaligen Kosten für die Entwicklung und das Training verbunden. Hinzu kommt die Notwendigkeit kontinuierlicher Verbesserungen und möglicher Adaptionen an neuere Entwicklungen. Das erzeugt insgesamt deutlich höhere Kosten im Vergleich zur Nutzung bestehender Modelle.
- Es ist unklar, wie hoch die Erfolgs- und Nutzenaussichten eines solchen LLMs am Ende sind. Insbesondere unter der Beachtung, dass es sich um einen sehr dynamischen Markt handelt, und die Innovationszyklen der Technologie sehr kurz sind.
- Schließlich muss abgewogen werden, wie die (begrenzten) Ressourcen verteilt werden. Bei einem solchen Projekt besteht die Gefahr, dass diese auch von bestehenden, erfolgreichen (Open-Source-)Projekten abgezogen und jene damit geschwächt werden.

Empfehlung: Die Bundesregierung sollte schnell evaluieren, ob ein eigenständiges Open-Source-LLM gewünscht und realisierbar ist. Bei einer positiven Entscheidung bedarf es einer schnellen Umsetzung, um vollumfänglich in den Innovationsprozess mit den erwartbaren positiven Externalitäten einzusteigen. Die Umsetzung sollte hohe Datenschutz- und Informationssicherheitsniveaus anstreben und in enger Abstimmung mit europäischen Partnern und Initiativen erfolgen. Parallel dazu sollten bestehende Open-Source-Modelle gezielt weiter genutzt, angepasst und mit staatlichen Anforderungen abgeglichen werden.

8.2.2 An Open-Source Ökosystemen partizipieren

Dimension: Strategisch, organisatorisch, technisch
Zeithorizont: Kurzfristig
Ziel: Das LLM-Open-Source-Ökosystem stärken und die Anschlussfähigkeit für die öffentliche Verwaltung verbessern

Einordnung: Open-Source-Angebote sind eine tragfähige Alternative zu proprietären Angeboten. Sie ermöglichen mehr Kontrolle, Transparenz und Anpassbarkeit und sind somit wichtiger Baustein digitaler Souveränität. Die Bundesverwaltung sollte nicht nur gezielt bestehende, erprobte Ökosysteme finanziell unterstützen, sondern zu diesen auch aktiv beitragen (z. B. auch Bereitstellung von unkritischen Entwicklungen für die öV). Eine strategische Beteiligung an bestehenden Open Source Communities ermöglicht langfristigere Einflussmöglichkeiten auf die Weiterentwicklung.

Vorgehensweise: Die öffentliche Hand sollte gezielt Ressourcen einsetzen, um Open-Source-Projekte mit Bezug zu LLMs strategisch zu fördern. Dies umfasst sowohl finanzielle Unterstützung als auch personelle Beiträge (z. B. durch Mitarbeit an Open-Source-Projekten). Ziel ist es, Teil der relevanten Open Source Communities zu werden, um bei Bedarf auch Einfluss auf die Entwicklungsrichtung nehmen zu können. Gleichzeitig sollte die Bundesverwaltung dafür sorgen, dass ihre Beschaffungs- und Projektstrukturen die Nutzung und Integration solcher Lösungen auch praktisch ermöglichen – etwa durch angepasste Vergabekriterien, Schnittstellenförderung und Know-how-Aufbau.

Vorteile:

- Die aktive Unterstützung von OSS-Projekten hilft, diese am Leben zu erhalten, zu pflegen und beständig an die sich wandelnden Bedarfe anzupassen. Damit verbunden sind alle Vorteile, die OSS bietet: So können Vendor Lock-ins durch adäquate alternative offene Software und offene Standards vermieden werden. Außerdem besteht die Möglichkeit zur unabhängigen Weiterentwicklung oder zum sicheren Betrieb in eigenen Infrastrukturen.

Risiken:

- Nicht immer kann auf die OSS-Lösung zurückgegriffen werden, unter Umständen fließen also Ressourcen in Projekte, die dann nicht genutzt werden. So kann es sein, dass Open-Source-Lösungen unter Umständen weniger leistungsfähig als proprietäre Angebote sind und eigene Prüfprozesse erfordern, da es keine Anbieterzusicherungen gibt. Gute proprietäre Lösungen mit klaren Verträgen können im Einzelfall eine bessere Balance aus Leistung, Sicherheit und Kontrolle bieten.

Empfehlung: Die Bundesregierung sollte sich aktiv und strukturiert an der Weiterentwicklung von Open-Source-Anwendungen mit Bezug zu LLMs beteiligen – finanziell, organisatorisch und (mittelbar) technisch. Um langfristig Einfluss auf zentrale technische und ethische Standards zu nehmen, sollte Deutschland sich zudem in relevanten Open-Source-Allianzen und -Konsortien sichtbar engagieren.

8.3 Rechtliche Vorgaben

8.3.1 Einen verpflichtenden Souveränitätscheck bei Projekten ab gewisser Kritikalität einführen

Dimension: Rechtlich
Zeithorizont: Kurzfristig
Ziel: Entwicklung und Einführung eines standardisierten Souveränitätschecks zur Bewertung von LLM-gestützten Systemen in der Bundesverwaltung

Einordnung: Derzeit fehlt in der Bundesverwaltung ein einheitliches, rechtlich fundiertes Bewertungsverfahren, um bei Projekten mit Einsatz großer Sprachmodelle systematisch die digitale Souveränität zu prüfen. Das »Zentrum für Digitale Souveränität der Öffentlichen Verwaltung« (ZenDiS) hat angekündigt, einen sogenannten Souveränitätscheck in Zukunft anbieten zu wollen. Ein verpflichtender »Souveränitätscheck« für Projekte ab einer gewissen Kritikalität (Größe, anvisierte Zielgruppe, Risiko) könnte frühzeitig Gefahren für die digitale Souveränität identifizieren. Dabei darf sich die Prüfung nicht allein auf das LLM beschränken, sondern muss den Gesamtkontext des Einsatzes – inklusive Dateninfrastruktur, Software-Stacks, Betriebs- und Governance-Strukturen – mit einbeziehen.

Vorgehensweise: Aufbauend auf Vorarbeiten ist ein standardisiertes Prüfschema zu entwickeln, das je nach Projektumfang verpflichtend anzuwenden ist – etwa ab einer bestimmten Projektgröße oder strategischen Bedeutung. Der Souveränitätscheck sollte sich modular anpassen lassen und klare Kriterien enthalten, die auch mit bestehenden Richtlinien (z. B. Cloud-Strategie, Datenschutzfolgenabschätzung) abgestimmt sind. Dabei ist auch die Orientierung an weiteren Kriterienkatalogen möglich, beispielsweise aus dieser Studie.

Vorteile:

- Eine Früherkennung möglicher Souveränitätsrisiken bei KI-gestützten Projekten führt zur Vermeidung unnötiger Folgekosten, z. B. unangemessene Preisforderungen kommerzieller Anbieter oder Umstiegskosten aufgrund wirtschaftlicher oder politischer Änderungen.
- Die Bewertung durch einen Souveränitätscheck bietet eine transparente Entscheidungsgrundlage für Vergaben und den Technologieeinsatz.

– Projektleitungen bekommen eine klare Orientierung an die Hand, die Unsicherheiten bezüglich Souveränitätsauswirkungen messbar macht und Risiken einschätzbar.

Risiken:

– Es existiert ein zusätzlicher Prüfaufwand in der Projektumsetzung, der zu Verzögerungen in der Entwicklung führen kann.

Empfehlung: Die Bundesregierung sollte kurzfristig die Einführung eines verpflichtenden Souveränitätschecks für LLM-gestützte Projekte in der Bundesverwaltung mit einer festzulegenden Mindestgröße initiieren. Dieser Check sollte gemeinsam mit relevanten Stakeholdern konzipiert und pilothaft getestet werden. Ziel ist ein praxistaugliches, rechtlich abgesichertes Verfahren, das als verpflichtender Bestandteil in die Planung, Vergabe und Bewertung von KI-gestützten Vorhaben integriert wird – insbesondere bei Projekten mit hoher Tragweite für Verwaltung und Gesellschaft.

8.3.2 Marktmacht stärken

Dimension: Strategisch
Zeithorizont: Mittelfristig
Ziel: Eine koordinierte, föderal übergreifende Bündelung der Beschaffung nach KI-Software und -Hardware zur Stärkung der Verhandlungsposition der öffentlichen Verwaltung und einheitlichen Berücksichtigung von Souveränitätsaspekten

Einordnung: Die Beschaffung erfolgt in der öffentlichen Verwaltung bislang häufig dezentral und unkoordiniert. Dadurch entstehen Insellösungen, Doppelstrukturen und eine geschwächte Verhandlungsposition gegenüber marktbeherrschenden Anbietern. Gleichzeitig fehlt es an strukturellen Anreizen zur angemessenen Bewertung vertrauenswürdiger, europäischer Alternativen. Eine strategische Bündelung der Beschaffung – über föderale Ebenen hinweg – kann zur Stärkung digitaler Souveränität beitragen und europäische Anbieter fördern, ohne gegen vergaberechtliche Grundsätze zu verstoßen.

Vorgehensweise: Es sollten bestehende Beschaffungsmechanismen auf Bundes-, Landes- und kommunaler Ebene analysiert und Möglichkeiten für eine zentrale oder föderal koordinierte IT-Beschaffung identifiziert und umgesetzt werden – etwa über gemeinsame Rahmenverträge oder Einkaufsgemeinschaften. In Vergabeverfahren können klare, transparente Kriterien zur Bewertung der digitalen Souveränität integriert werden. Gleichzeitig sollten konkrete Handreichungen für Beschaffungsstellen entwickelt werden, die die rechtssichere Berücksichtigung von Souveränitätsaspekten ermöglichen, ohne das Gebot der Gleichbehandlung zu verletzen.

Vorteile:

– Ein zentraler Vorteil gemeinsamer Beschaffung ist die Vermeidung unkoordinierter Insellösungen und unwirtschaftlicher Mehrfachbeschaffungen.
– Gemeinsame und damit zumeist größere Beschaffungsvorhaben stärken die Verhandlungsposition der öffentlichen Verwaltung gegenüber Anbietern.
– Es kann davon ausgegangen werden, dass die Bündelung zu einer höheren Effizienz, Transparenz und Standardisierung in der Beschaffung führt. Das ist auch für die Wirtschaft interessant, die sich an diesen Standards orientieren kann und gezielt auf die Bedarfe des öffentlichen Sektors zugeschnittene Angebote entwickelt.

Risiken:

– Verfahren müssen rechtssicher gestaltet werden, um das Gleichbehandlungsgebot im Vergaberecht nicht zu verletzen.
– Es ist von einem hohen Initialaufwand beim Aufbau gemeinsamer Vergabestrukturen auszugehen.

Empfehlung: Die Bundesregierung sollte mittelfristig eine koordinierte Beschaffungsstrategie für KI-Produkte und -Infrastrukturen initiieren, die föderale Synergien nutzt und auf die Stärkung digitaler Souveränität ausgerichtet ist. Dazu zählen die Entwicklung souveränitätsbezogener Bewertungskriterien, die Erstellung praxisnaher Leitlinien für Vergabestellen sowie die Förderung gemeinsamer Rahmenverträge. Ziel ist es, die Marktmacht der öffentlichen Verwaltung gezielt zu nutzen, um souveräne, europäische Alternativen zu fördern und langfristige technologische Abhängigkeiten zu reduzieren.

8.4 Weitere Maßnahmen

8.4.1 DE-/EU-fokussierte Trainingsdaten definieren, erstellen und aktuell halten

Dimension: Technisch
Zeithorizont: Mittelfristig
Ziel: Aufbau und Pflege qualitativ hochwertiger, DSGVO-konformer Trainingsdaten mit Fokus auf europäische Werte, kulturelle Besonderheiten und rechtliche Normen

Einordnung: Trainingsdaten sind die Grundlage von LLMs und haben maßgeblichen Einfluss auf deren Output. Derzeit basieren viele LLMs auf überwiegend US-amerikanischen oder global aggregierten Datensätzen, was kulturelle Verzerrungen, rechtliche Unstimmigkeiten und eine mangelnde Berücksichtigung europäischer Werte und Normen zur Folge haben kann. Um dem Risiko einer kulturellen Überformung oder unbeabsichtigten inhaltlichen Beeinflussung entgegenzuwirken, ist die Entwicklung und Pflege europäisch geprägter Trainingsdaten interessant.

Vorgehensweise: Es sollte ein strukturierter europäischer Datenraum aufgebaut werden, der qualitativ hochwertige, DSGVO-konforme Text- und Wissensdaten umfasst. Diese Daten sollten in Form kuratierter, offener oder geschützter Datenpools bereitgestellt werden, etwa aus öffentlichen Quellen (Verwaltungsportale, Gesetzestexte, Bildungsinhalte), qualitätsgesicherten Medien und ergänzt möglicherweise durch geeignete synthetische Daten. Wichtig ist dabei eine klare Definition, was unter »europäischen« Daten verstanden wird – in rechtlicher, kultureller und sprachlicher Hinsicht. Zusätzlich müssen Mechanismen etabliert werden, um diese Daten aktuell zu halten, Fehlentwicklungen frühzeitig zu erkennen und Rückkopplungsschleifen mit der KI-Forschung zu ermöglichen.

Vorteile:

- Ein zentraler Vorteil ist, dass davon auszugehen ist, dass die pro-europäische LLM-Entwicklung von einem solchen Datensatz profitieren würde. Ein solcher Datensatz bildet das Fundament für wertgeleitete europäische KI-Systeme: Die Ergebnisse von Modellen, die darauf trainiert werden, wären spezifischer für den europäischen Kontext geeignet. Unter anderem steigt damit die Vertrauenswürdigkeit in die Systeme, es lässt sich Datenschutz gewährleisten und damit eine rechtliche Konformität des Trainingsprozesses.
- Über LLMs hinausgehend bedeutet ein solcher Datensatz die Schaffung einer strategischen Ressource für souveräne Technologieentwicklung und -innovation in Europa.

Risiken:

- Aufbau, Qualitätssicherung und Pflege entsprechender Datenräume ist mit hohem Ressourcenaufwand verbunden.
- Im Umgang mit Internetdaten liegt eine Herausforderung in der Abgrenzung, was als international, spezifisch europäisch oder national gilt. Entsprechend kann es zu Entscheidungsschwierigkeiten kommen, welche Daten tatsächlich Teil eines solchen Datenraums sind.
- Es bedarf erhöhten Abstimmungsbedarfes mit bestehenden europäischen Dateninfrastrukturprojekten (z. B. GAIA-X, European Language Data Space).

Empfehlung: Die Bundesregierung sollte sich für den Aufbau eines europäischen Trainingsdatenraumes starkmachen, der auch den Verwaltungskontext berücksichtigen muss. Dies sollte in enger Abstimmung mit europäischen Initiativen, Forschungseinrichtungen und Open-Data-Projekten erfolgen. Parallel sollten Definitionen für »europäische Trainingsdaten« erarbeitet sowie Anreize zur Bereitstellung und Kuratierung hochwertiger Daten geschaffen werden. Ziel ist ein europäischer Datenpool, der auch die Grundlage für souveräne KI-Systeme bildet.

8.4.2 Positive Narrative zum Einsatz von KI in der öffentlichen Verwaltung entwickeln

Dimension: Strategisch
Zeithorizont: Kurzfristig
Ziel: Die Entwicklung gemeinsamer Zielbilder und positiver Narrative soll die Handlungsfähigkeit von Verwaltungen im Umgang mit LLMs stärken und eine aktive Auseinandersetzung mit den Chancen, Grenzen und Wirkungen ermöglichen.

Einordnung: Die Einführung und Nutzung von KI in der öffentlichen Verwaltung ist nicht allein eine technische oder rechtliche Frage, sondern auch eine kulturelle. Häufig bestehen Unsicherheiten, Unklarheiten über Nutzen und Zielrichtung von KI-Projekten oder eine eher defensive Haltung, was zusammengefasst als ein negatives Mindset beschrieben werden kann. Das Mindset ist neben Fähigkeiten und Können eine Dimension von Kompetenz (Kupi et al. 2025) und zahlt damit direkt auf das Souveränitätsziel *Gestaltungsfähigkeit* ein. Narrative können eine Veränderung im Mindset bewirken, indem sie Orientierung geben und zur Mitgestaltung motivieren.

Vorgehensweise: In einem ersten Schritt sollten in ausgewählten Verwaltungen partizipative Prozesse zur Entwicklung von Zukunfts- und Leitbildern angestoßen werden – z. B. über Workshops, interne Diskursformate, Beteiligungsinstrumente und verbindende Foresightprozesse. Parallel sollten Best Practices aus laufenden oder erfolgreich abgeschlossenen KI-Projekten systematisch gesammelt, sichtbar gemacht und in verständlicher Sprache aufbereitet werden. Diese Praxisbeispiele können intern wie extern als positive Anker und Referenzen dienen.

Vorteile:

- Positive Narrative zahlen auf die Überwindung kultureller Barrieren gegenüber KI in der Verwaltung ein und tragen damit zur Akzeptanz bei.
- Ein gemeinsames, als positiv empfundenes Zielbild stärkt Motivation, Identifikation und Engagement bei Mitarbeitenden.

Risiken:

- Es besteht bei dieser Empfehlung die Gefahr, dass das Thema als »kommunikative Fingerübung« ohne Wirkung wahrgenommen wird. Das ist zwar kein unmittelbares Risiko für digitale Souveränität, allerdings sind dann weniger positive Effekte zu erwarten.

Empfehlung: Die Bundesregierung sollte kurzfristig Maßnahmen zur Förderung positiver KI-Narrative – möglicherweise aufbauend auf den im KI-Leitbild formulierten »wertebasierten Leitprinzipien als gemeinsame Handlungsgrundlage« (Bundesministerium des Innern (BMI) 2025a) – in der Verwaltung

anstoßen, etwa in geeigneten Formaten (z. B. Diskursimpulse, Kommunikationsbausteine, Workshops) sowie durch die systematische Aufarbeitung von Best Practices. Mittelfristig sollten narrative Zielbilder ein fester Bestandteil strategischer KI-Planung innerhalb der öffentlichen Verwaltung und aktiv in Transformationsprozesse eingebunden werden.

8.4.3 Proof-of-Concept: Zusammenarbeit zwischen wissenschaftlichen KI-Kompetenzzentren und der öffentlichen Verwaltung verstärken

Dimension: Organisatorisch
Zeithorizont: Kurzfristig
Ziel: Die gezielte Kooperation zwischen der öffentlichen Verwaltung und den vom BMFTR geförderten KI-Kompetenzzentren soll dazu beitragen, zentrale Herausforderungen der Verwaltungspraxis direkt zu adressieren.

Einordnung: In Deutschland bestehen bereits mehrere exzellent aufgestellte KI-Kompetenzzentren mit starker internationaler Vernetzung und wissenschaftlicher Expertise. Diese arbeiten an fortschrittlichen KI-Lösungen – bislang aber teilweise ohne systematische Anbindung an konkrete Bedarfe der öffentlichen Verwaltung. Durch eine gezielte, institutionalisierte Zusammenarbeit können wissenschaftliche Forschung und verwaltungsspezifische Anwendungsfälle enger zusammengebracht werden. Dies erhöht sowohl die Relevanz und Wirkung öffentlicher Forschung als auch die Innovationsfähigkeit der Verwaltung. Gleichzeitig wird die Grundlage für vertrauenswürdige, an europäische Werte angelehnte LLM-Systeme gestärkt.

Vorgehensweise: Es sollte ein gemeinsames Proof-of-Concept (PoC) zwischen öffentlichen Stellen (z. B. Bundesbehörden, Länder, Kommunen) und wissenschaftlichen KI-Kompetenzzentren initiiert werden. Dieses Projekt sollte ein oder mehrere praxisrelevante Verwaltungsprobleme adressieren und auf die Entwicklung anwendungsorientierter, nachvollziehbarer und diskriminierungsfreier KI-Lösungen abzielen. Neben Pilotierungen sollten auch begleitende Forschungsformate, Nachwuchsförderung sowie der Austausch von Fachpersonal (z. B. über Fellowships oder Co-Innovation Labs) gefördert werden. Die Ergebnisse könnten perspektivisch in Open-Source-Lösungen und Ausgründungen überführt werden.

Vorteile:

- Ein großer Vorteil ist die Stärkung des gegenseitigen Transfers von Wissen zwischen Forschung und Verwaltungspraxis. Dadurch gelänge eine bessere Nutzung wissenschaftlicher Expertise für konkrete Verwaltungsherausforderungen.
- Nach einem erfolgreichen PoC ließen sich langfristigere Partnerschaften zwischen Wissenschaft und Verwaltung aufbauen. Erfolgreiche Lösungen könnten z. B. zu Ausgründungen führen und so das nnovationspotenzial stärken.

Risiken:

- Risiken liegen unter anderem in unterschiedlichen Zeithorizonten und Zielsystemen von Wissenschaft und Verwaltung. Wenn diese nicht in Einklang gebracht werden, können Zusammenarbeiten scheitern.
- Es besteht die Gefahr, dass sich PoCs als punktuelle Einzelprojekte ohne nachhaltigere Strukturwirkung herausstellen.

Empfehlung: Die Bundesregierung sollte eine strukturelle Zusammenarbeit in Form eines PoC mit den vom BMFTR geförderten KI-Kompetenzzentren anstoßen und perspektivisch institutionalisieren. Ziel ist der Aufbau langfristiger Partnerschaften und Innovationsnetzwerke, die wissenschaftliche Expertise gezielt in die Entwicklung vertrauenswürdiger LLM-Anwendungen für die öffentliche Verwaltung einbringen. Dazu sollten ressortübergreifende Pilotprojekte, koordinierte Förderformate und gemeinsame Austauschplattformen entwickelt werden.

8.4.4 KI-Trends kontinuierlich beobachten

Dimension: Strategisch
Zeithorizont: Kurzfristig
Ziel: Systematische Beobachtung und Bewertung neuer KI-Trends, um deren Potenziale und Risiken frühzeitig für die öffentliche Verwaltung einschätzen zu können

Einordnung: Die Entwicklung von KI – insbesondere bei LLMs – ist durch hohe Dynamik und kurze Innovationszyklen gekennzeichnet. Für die öffentliche Verwaltung ist es entscheidend, technologische Entwicklungen frühzeitig zu erkennen, ihre Relevanz realistisch zu bewerten und daraus strategische Handlungsoptionen abzuleiten sowie mögliche Einflüsse auf die digitale Souveränität einzuschätzen. Dies betrifft nicht nur neue Modellarchitekturen oder Anbieter, sondern auch strukturelle Entwicklungen wie KI-Middleware, agentenbasierte Systeme oder neue Paradigmen wie föderiertes bzw. »verbündetes« Lernen. Ein kontinuierliches Technologie-Monitoring kann helfen, Chancen gezielt zu nutzen und Fehlentwicklungen zu vermeiden.

Vorgehensweise: Es sollte eine institutionalisierte Beobachtungseinheit aufgebaut werden, die technologische KI-Entwicklungen regelmäßig analysiert und bewertet. Dazu gehören:

- Marktanalysen, z. B. zur Entwicklung von KI-Middleware-Plattformen oder offenen Modell-Ökosystemen
- Technologiebewertung, z. B. zu Ansätzen wie »verbündetes Lernen«, multimodalen Modellen oder Toolformer-Systemen
- Trendanalysen, z. B. zu KI-Agenten, selbstorganisierenden Systemen oder globalen Governance-Fragen

Die Ergebnisse sollten in regelmäßige Berichte einfließen, die praxisnah für Verwaltungen aufbereitet werden und strategische Empfehlungen ableiten – z. B. für Pilotierungen, Förderungen oder regulatorische Abwägungen.

Vorteile:

- Vorausschau in einem hochdynamischen Technologiefeld ermöglicht das frühzeitige Erkennen von strategisch relevanten technischen Entwicklungen und bietet somit Orientierung. Diese Orientierung hilft, kurzfristige Fehlentscheidungen durch vorschnelle Adaption oder Hype-Getriebenheit zu vermeiden.
- Das Erkennen von Trends kann (nationale) Innovationsfähigkeit – und damit indirekt die digitale Souveränität – stärken, indem frühzeitig relevante Projekte bzw. Anbieter gefördert werden können.

Risiken:

- Es besteht stets auch das Risiko von Fehleinschätzungen durch unklare Reifegrade, komplexe Dynamiken, Sprunginnovationen oder begrenzte Anwendbarkeit auf Verwaltungskontexte.
- Für verlässliche und kompetente Vorausschau ist ein hohes Maß an technischer Expertise erforderlich. Das macht den Aufbau entsprechender Kompetenzen notwendig und ist mit Kosten verbunden. Die Wirtschaftlichkeit solcher Maßnahmen ist nicht unbedingt unmittelbar ersichtlich.

Empfehlung: Die Bundesregierung sollte eine kontinuierliche, fachlich fundierte Beobachtung und Bewertung neuer KI-Trends etablieren, idealerweise in Kooperation mit Forschungseinrichtungen, europäischen Partnern und bestehenden Gremien der IT-Steuerung. Die gewonnenen Erkenntnisse sollten in strukturierter Form für die strategische Planung, Projektbewertung und Technologiesouveränität der öffentlichen Verwaltung nutzbar gemacht werden. So kann gewährleistet werden, dass die Verwaltung technologische Entwicklungen nicht nur nachvollzieht, sondern auch rechtzeitig mitgestalten kann.

Literaturverzeichnis

Bitkom (Hg.) (2025): Digitale Souveränität 2025. Wie abhängig ist unsere Wirtschaft? https://www.bitkom.org/sites/main/files/2025-02/2025-bitkom-studienbericht-digitale-souveraenitaet.pdf.

Bundesministerium des Innern und für Heimat (BMI) (Hg.) (2025a): Leitlinien für den Einsatz Künstlicher Intelligenz in der Bundesverwaltung. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/moderne-verwaltung/ki/BMI25020-leitlinien-ki-bundesverwaltung.pdf?__blob=publicationFile&v=3.

Bundesministerium des Innern und für Heimat (BMI) (Hg.) (2025b): Marktplatz der KI-Möglichkeiten. https://maki.beki.bund.de/a/bmi-makimo-app.

Bundesministerium für Digitales und Verkehr (BMDV) (Hg.) (2023): Nationale Datenstrategie beschlossen. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2023/datenstrategie.html.

Capgemini (2025): Data foundations for government. Online verfügbar unter https://www.capgemini.com/wp-content/uploads/2025/05/Capgemini-Research-Institute-report_Data-foundations-for-government_From-AI-ambition-to-execution-2.pdf.

CDU; CSU; SPD (Hg.) (2025): Verantwortung für Deutschland. Koalitionsvertrag zwischen CDU, CSU und SPD. 21. Legislaturperiode. Online verfügbar unter https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag2025_bf.pdf.

CIO Bund (2023): Künstliche Intelligenz in der Verwaltung. In: Der Beauftragte der Bundesregierung für Informationstechnik, 02.11.2023. Online verfügbar unter https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/datenpolitik/daten-und-ki/daten-und-ki-node.html.

Deloitte (2021): Analyse der Abhängigkeit der Öffentlichen Verwaltung von Datenbankprodukten. Online verfügbar unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/abschlussbericht-datenbankanalyse.pdf?__blob=publicationFile&v=5.

Deutsche Bank Research (2024b): Latest in AI: Copilot+ PCs, AI Safety Summit, EU AI Act, and »AI factories«. Online verfügbar unter https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000533704/Latest_in_AI%3A_Copilot%2B_PCs%2C_AI_Safety_Summit%2C_EU_A.PDF?&undefined&reaload=IA/iXbxGpWqA/fHJA85yw/V4Gyl7ewzEVXcJH~rP2gYIEBvluW7Y/AGQhATwooti.

Deutsche Bank Research (2024a): Nukleare Option, Nobelpreis, KI im Finanzwesen, AMD vs. Nvidia. Online verfügbar unter https://www.dbresearch.de/PROD/RPS_DE-PROD/PROD0000000000536247/Neues_aus_KI%3A_Nukleare_Option%2C_Nobelpreis%2C_KI_im_F.PDF?&undefined&realload=vTV0x4ZMp7FyUFY6CCW114VpoDQQAbjlIrT/UylfrPpwJpd4isXBLuDsjF1p6vPf.

Deutscher Bundestag (Hg.) (2024): Schriftliche Fragen mit den in der Woche vom 4. November 2024 eingegangenen Antworten der Bundesregierung. Drucksache 20/13684.

Dipartimento per la transformazione digitale (2024): Italian strategy for artificial intelligence 2024–2026. Online verfügbar unter https://www.agid.gov.it/sites/agid/files/2024-07/Italian_strategy_for_artificial_intelligence_2024-2026.pdf.

Epoch AI (2025): Notable AI Models. Online verfügbar unter https://epoch.ai/data/notable-ai-models.

Fernandez, Joaquin (2025): The leading generative AI companies. Hg. v. IoT Analytics. Online verfügbar unter https://iot-analytics.com/leading-generative-ai-companies/.

Fontana, Susanna; Errico, Beatrice; Tedesco, Sara; Bisogni, Fabio; Renwick, Robin; Akagi, Mikio; Santiago, Nicole (2024): AI and GenAI adoption by local and regional administrations: Publications Office of the European Union. Online verfügbar unter https://op.europa.eu/en/publication-detail/-/publication/40363d58-bdc8-11ef-91ed-01aa75ed71a1/language-en.

Gartner (2017): Gartner Magic Quadrant for Cloud Infrastructure as a Service, Worldwide. Online verfügbar unter https://www.gartner.com/en/documents/3738058.

Goldacker, Gabriele (2017): Digitale Souveränität. Online verfügbar unter https://www.oeffentliche-it.de/publikationen/digitale-souveraenitaet/.

Gouvernement (2021): STRATÉGIE NATIONALE POUR L'INTELLIGENCE ARTIFICIELLE. Online verfügbar unter https://www.enseignementsup-recherche.gouv.fr/sites/default/files/2021-11/dossier-de-presse---strat-gie-nationale-pour-l-intelligence-artificielle-2e-phase-14920.pdf.

Government, Australian (2024): National framework for the assurance of artificial intelligence in government. Online verfügbar unter https://www.finance.gov.au/sites/default/files/2024-06/National-framework-for-the-assurance-of-AI-in-government.pdf.

Holzki, Larissa (2025): Diese Firma will KI bis zu 400 Prozent leistungsfähiger machen. Aleph Alpha. Hg. v. Handelsblatt. Online verfügbar unter https://www.handelsblatt.com/technik/ki/aleph-alpha-diese-firma-will-ki-bis-zu-400-prozent-leistungsfaehiger-machen/100101975.html.

Horstmann, Jutta (2024): Stellungnahme Anhörung »Open Source« im Ausschuss für Digitales. Hg. v. Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS). Online verfügbar unter https://admin.zendis.de/wp-content/uploads/2024_12_04-Stellungnahme-ZenDiS-Anhoerung-Open-Source-Digitalausschuss.pdf.

Intel Market Research (2024): Large Language Model (LLM) Market Growth Analysis, Market Dynamics, Key Players and Innovations, Outlook and Forecast 2024-2030. Online verfügbar unter https://www.linkedin.com/pulse/large-language-model-llm-market-growth-analysis-wfjef/.

IT-Planungsrat (Hg.) (2021): Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung. Strategische Ziele, Lösungsansätze und Maßnahmen zur Umsetzung. Beschluss 2021/09. Online verfügbar unter https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf.

ITZBund (2024): KIPITZ – Das KI-Portal des ITZBund. Online verfügbar unter https://egovernmentwettbewerb.de/wp-content/uploads/2024/07/ITZ_Bund_KIPITZ_Kat_1.pdf.

Korinek, Anton; Vipra, Jai (2024): Market Concentration Implications of Foundation Models: The Invisible Hand of ChatGPT. Online verfügbar unter https://www.economic-policy.org/wp-content/uploads/2024/03/EcPol-2023-183.R1_Proof_hi_Korinek_Vipra.pdf.

Kupi, Maximilian; Goldacker, Gabriele; Wachsmann, Dorian (2025): Kompetenzen für den Einsatz generativer Künstlicher Intelligenz in der Verwaltung. Hg. v. Kompetenzzentrum Öffentliche IT. Online verfügbar unter https://www.oeffentliche-it.de/publikationen/kompetenzen-fuer-den-einsatz-generativer-kuenstlicher-intelligenz/.

Mohabbat Kar, Resa; Thapa, Basanta E. P. (2020): Digitale Souveränität als strategische Autonomie. Umgang mit Abhängigkeiten im digitalen Staat. 1. Auflage. Berlin: Kompetenzzentrum Öffentliche IT Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS. Online verfügbar unter https://www.oeffentliche-it.de/publikationen/digitale-souveraenitaet-als-strategische-autonomie-umgang-mit-abhaengigkeiten-im-digitalen-staat/.

MPK (2025): Technologische Souveränität sichern – KI-Standorte Europa und Deutschland stärken. Online verfügbar unter https://www.ministerpraesident.sachsen.de/ministerpraesident/07_TOP2_Beschluss_MPK_RS.pdf.

Naveed, Humza; Khan, Asad Ullah; Qiu, Shi; Saqib, Muhammad; Anwar, Saeed; Usman, Muhammad et al. (2023): A Comprehensive Overview of Large Language Models. Online verfügbar unter https://arxiv.org/abs/2307.06435.

Office of Management and Budget (2024): M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence. Online verfügbar unter https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.

Open Source Initiative (2024): The Open Source AI Definition – 1.0. Online verfügbar unter https://opensource.org/ai/open-source-ai-definition.

oxfordinsights (2024): Government AI Readiness Index 2024. Online verfügbar unter https://oxfordinsights.com/ai-readiness/ai-readiness-index/.

Papers With Code (2025): Multi-task Language Understanding on MML. Online verfügbar unter https://paperswithcode.com/sota/multi-task-language-understanding-on-mmlu.

PwC (2019): Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern. Online verfügbar unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/marktanalyse-reduzierung-abhaengigkeit-software-anbieter.pdf

SDAIA (2020): National Strategy for Data & AI. Online verfügbar unter https://sdaia.gov.sa/en/SDAIA/SdaiaStrategies/Pages/NationalStrategyForDataAndAI.aspx.

Sowe, Sulayman; Mou, Yongli; Cheng, Du; Kong, Lingxiao; Neumann, Alexander Tobias; Decker, Stefan (2024): Understanding Open Source Large Language Models: An Exploratory Study. In: 2024 2nd International Conference on Foundation and Large Language Models (FLLM). 2024 2nd International Conference on Foundation and Large Language Models (FLLM). Dubai, United Arab Emirates, 26.11.2024–29.11.2024: IEEE, S. 132–140.

Steer, Alissa Theresa; Pohle, Julia (2024): Digitale Souveränität. bidt. Online verfügbar unter https://www.bidt.digital/glossar/digitale-souveraenitaet/?ref=map.

Teadusministeerium; Justiitsmiinisteerium (2024): Tehisintellekti tegevuskava 2024-2026. Online verfügbar unter https://www.kratid.ee/_files/ugd/7df26f_21000a2dd36c4a66a30eea97563370a3.pdf.

Thun, Max von; Hanley, Daniel A. (2024): Stopping Big Tech from Becoming Big AI. Online verfügbar unter https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/6710039559ef840f59365bc8/1729102742546/Stopping+Big+Tech+from+Becoming+Big+AI.pdf.

Uspenskyi, Serhii (2025): Large Language Model Statistics And Numbers. Hg. v. Springs. Online verfügbar unter https://springsapps.com/knowledge/large-language-model-statistics-and-numbers-2024.

Verordnung (EU) 2024/1689: Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz). Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R1689.

Wachsmann, Dorian; Weber, Mike (2025): ThemenRadar 2025. Digitalthemen in der öffentlichen Verwaltung 2025. ÖFIT. Online verfügbar unter https://www.oeffentliche-it.de/umfragen/themenradar-2025/.

Weng, Lilian (2023): LLM Powered Autonomous Agents. Online verfügbar unter https://lilianweng.github.io/posts/2023-06-23-agent/.

White, Matt; Haddad, Ibrahim; Osborne, Cailean; Liu, Xiao-Yang Yanglet; Abdelmonsef, Ahmed; Varghese, Sachin; Le Hors, Arnaud (2024): The Model Openness Framework: Promoting Completeness and Openness for Reproducibility, Transparency, and Usability in Artificial Intelligence. Online verfügbar unter https://arxiv.org/abs/2403.13784.

Anhang

A.1 Erhebungsbogen

PDF des Erhebungsbogens zu finden unter: oeffentliche-it.de

A.2 Liste der Marktanalysen

Herausgeber	Jahr	Dokument
USD Analytics	2025	Large Language Model (LLM) Market Size, Share, Trends, Growth Outlook, and Opportunities to 2034- By Type (Hundreds of Billions of Parameters, Trillions of Parameters), By Function (Custom Service, Content Generation, Sentiment Analysis, Code Generation, Chatbots and Virtual Assistant, Language Translation), By Deployment (Cloud, On-Premises), By Modality (Code, Video, Text, Image), By Product (Domain-Specific LLM Software, General-Purpose LLM Software, Services), By End-User (Medical, Financial, IT and ITES, Manufacturing, Education, Legal, Gaming, Media and Entertainment, Retail and e-commerce, Others), Countries and Companies Report; https://www.usdanalytics.com/industry-reports/large-language-model-market
Intel Market Research	2024	Large Language Model (LLM) Market Growth Analysis, Market Dynamics, Key Players and Innovations, Outlook and Forecast 2024-2030; https://www.linkedin.com/pulse/large-language-model-llm-market-growth-analysis-wfjef/
BIS Research	2024	Large Language Model (LLM) Market – A Global and Regional Analysis; https://bisresearch.com/industry-report/large-language-model-market.html
Research and Markets	2025	Large Language Model (LLM) Market Report 2025; https://www.researchandmarkets.com/reports/5989779/large-language-model-llm-market-report#product--summary
Research and Markets	2025	Large Language Model (LLM) Market Report: Trends, Forecast and Competitive Analysis to 2031; https://www.researchandmarkets.com/reports/5928828/large-language-model-llm-market-report#product--adaptive
MarketsandMarkets	2024	Large Language Model (LLM) Market; https://www.marketsandmarkets.com/Market-Reports/large-language-model-llm-market-102137956.html
DATAINTELO	2025	Large Language Model (LLM) Market; https://dataintelo.com/report/large-language-model-llm-market
Congruence Market Insights	2023	Large Language Model Market; https://www.congruencemarketinsights.com/report/large-language-model-market
Market Research Future	2025	Large Language Model Market; https://www.marketresearchfuture.com/reports/large-language-model-market-22213
Springs	2025	Large Language Model Statistics And Numbers; https://springsapps.com/knowledge/large-language-model-statistics-and-numbers-2024
Market.US	2025	Large Language Model (LLM) Market; https://market.us/report/large-language-model-llm-market/
Business Research Insights	2025	Large Language Model (LLM) Market; https://www.businessresearchinsights.com/market-reports/large-language-model-llm-market-117072
Grand View Research	o.J.	Large Language Models Market Size, Share & Trends Analysis Report; https://www.grandviewresearch.com/industry-analysis/large-language-model-llm-market-report
Verified Market Reports	2025	LLM -Markt für Großsprachenmodell; https://www.verifiedmarketreports.com/de/product/large-language-model-llm-market/

A.3 Analysierte Literatur Ausland

Land	Jahr	Dokument
Austria	2021	Strategie der Bundesregierung für Künstliche Intelligenz »AIM AT 2030«
Austria	2024	Praxisleitfaden für Digitale Verwaltung: KI, Ethik und Recht 2.0
Belgium	2022	Plan National de Convergence pour le Développement de l'Intelligence Artificielle
Belgium	2019	AI4Belgium – National AI Strategy (Report)
Canada	2019	Directive on Automated Decision-Making
Canada	2025	Artificial Intelligence Strategy for the Federal Public Service, 2025–2027
Canada	2025	Guide on the Use of Generative AI
South Korea	2019	National Strategy for Artificial Intelligence
South Korea	2020	Human-Centered AI Ethics Guidelines
South Korea	2024	Guidelines for Adoption and Utilisation of Large-Scale AI in the Public Sector
South Korea	2025	Framework Act on AI Development and Establishment of a Foundation for Trustworthiness
Singapore	2019	National AI Strategy (NAIS)
Singapore	2023	National AI Strategy 2.0
Denmark	2019	Danmarks Nationale Strategi for Kunstig Intelligens
Denmark	2023	Danmarks Digitaliseringsstrategi 2024–2027
Denmark	2024	Ny Strategisk Indsats for Kunstig Intelligens
Estonia	2019	Eesti Riiklik Tehisintellekti Strateegia 2019–2021
Estonia	2024	Tehisintellekti tegevuskava 2024–2026
Finland	2017	Tekoälyohjelma: Suomi – Tekoälyn Aikakaudelle
Finland	2020	AuroraAI – Kansallinen tekoälyohjelma
Finland	2020	Tekoälyn eettinen ohjeistus julkishallinnolle
Finland	2024	Generative AI Experiments in Public Administration
EU	2021	Proposal for a Regulation on Artificial Intelligence (AI Act)
EU	2021	Coordinated Plan on Artificial Intelligence (2021 Update)
EU	2020	Berlin Declaration on Digital Society and Value-Based Digital Government
France	2022	Artificial Intelligence and Public Action: Building Trust, Serving Performance
France	2025	Government Strategy for Deploying AI in the Public Sector
France	2025	Faire de la France une puissance de l'IA
France	2024	Strategy for the Use of AI in Human Resources Management of the State Civil Service
Germany	2025	Guidelines for the Use of Artificial Intelligence in the Federal Administration
Germany	2022	Voluntary Guidelines for AI Use in the Labor and Social Administration
Germany	2020	National Artificial Intelligence Strategy (Updated)
Ireland	2021	AI – Here for Good: National Artificial Intelligence Strategy
Ireland	2024	AI – Here for Good (Refresh 2024)
Ireland	2025	Guidelines for the Responsible Use of Artificial Intelligence in the Public Service
Ireland	2023	Cyber Security Guidance on Generative AI for Public Sector Bodies
Italy	2021	National Strategic Program on Artificial Intelligence 2022–2024
Italy	2024	Italian Strategy for Artificial Intelligence 2024–2026
Italy	2018	White Paper on Artificial Intelligence at the Service of the Citizen
Malaysia	2021	National Guidelines on AI Governance and Ethics
Malaysia	2024	AI at Work 2.0 Initiative
Malaysia	2025	AI at Work 2.0 Initiative
Netherlands	2019	Strategic Action Plan for Artificial Intelligence
Netherlands	2024	Government-wide Vision on Generative AI

Land	Jahr	Dokument
Netherlands	2022	Algorithm Register
UK	2021	National AI Strategy
UK	2023	Algorithmic Transparency Recording Standard – Guidance for Public Sector Bodies
UK	2025	Artificial Intelligence Playbook for the UK Government
Norway	2020	National Strategy for Artificial Intelligence
Norway	2024	National Digitalisation Strategy for the Public Sector 2024–2030
Norway	2023	Digdir's Guidance for Responsible AI Use in the Public Sector
Sweden	2018	National Approach for Artificial Intelligence
Sweden	2025	National Guidelines for the Use of Generative AI in Public Administration
Australia	2024	National Framework for the Assurance of Artificial Intelligence in Government
Australia	2024	Policy for the Responsible Use of AI in Government
Australia	2023	Interim Guidance on Generative AI for Government Agencies
Israel	2021	Government Decision No. 212 – Promoting Innovation and AI in the Public Sector
Israel	2023	Government Resolution No. 173 – National AI Program
Israel	2023	Israel's Policy on Artificial Intelligence – Regulation & Ethics
China	2017	New Generation Artificial Intelligence Development Plan
China	2022	SPC's Opinions on Regulating and Strengthening AI Applications in the Judiciary
China	2025	Implementation Opinion on Promoting High-Quality Development of the Data Labeling Industry
Taiwan	2023	Taiwan AI Action Plan 2.0
Taiwan	2023	Draft Guidelines for Generative AI Use in Government
Taiwan	2024	Draft Basic Act on Artificial Intelligence
Japan	2024	AI Business Operator Guidelines, v1.0
Japan	2024	Guidebook on Risk Countermeasures for Text-Generating AI (alpha)
Japan	2025	Draft Guidelines on Procuring and Utilizing Generative AI for Government Innovation
Saudi Arabia	2020	National Strategy for Data and AI (NSDAI)
Saudi Arabia	2023	Principles of AI Ethics
Saudi Arabia	2024	Generative AI Guidelines for the Government
UAE	2017	UAE National Strategy for Artificial Intelligence 2031
UAE	2022	AI Ethics Guidelines
UAE	2023	AI Adoption Guideline in Government Services
UAE	2023	Generative AI Guide: 100 Practical Applications and Use Cases
Deutschland	2023	BMBF – Aktionsplan Künstliche Intelligenz
Deutschland	2024	OECD – Bericht zu Künstlicher Intelligenz in Deutschland
Deutschland	2024	BSI – Secure, robust and transparent application of AI
Deutschland	2025	Kriterienkatalog des BSI zur Integration von extern bereitgestellten generativen KI-Modellen in eigene Anwendungen

A.4 Analyse der Strategien Deutschland und Ausland

Land	Investitionen in digitale Souveränität bei KI und LLMs	Digitale Souveränität & Risikobewusstsein	Governance & menschliche Kontrolle	Offenheit gegenüber ausländischen LLMs	Archetyp
Australien	Niedrig/Implizit – Keine klare Investition in souveräne LLMs; Abhängigkeit von öffentlichen Tools wie ChatGPT mit minimaler Entwicklung nationaler Fähigkeiten.	Hoch – Starke Warnungen gegen Datenexposition mit öffentlichen LLMs; hohe Übereinstimmung mit Datenschutz-/Sicherheitsstandards.	Sehr hoch – Klare »Human-in-the-loop«-Regeln, Transparenzvorschriften und Überwachung der KI-Nutzung in der Regierung.	Hoch – Offen für kommerzielle Tools wie ChatGPT und Bard; Richtlinien konzentrieren sich auf sichere Nutzung statt Einschränkung.	Pragmatisch
Belgien	Mäßig bis hoch – Investitionen in nationale Infrastruktur, »Deep Tech«-Fonds und Unterstützung interregionaler KI-Forschungskooperationen.	Hoch – Betonung des Datenschutzes, nationaler Infrastruktur und Integration von KI mit Cybersicherheits- und Datenschutzmaßnahmen.	Sehr hoch – Starke ethische Rahmenbedingungen, Transparenz, Maßnahmen gegen Vorurteile und ein vorgeschlagenes Governance-Gremium für die KI-Aufsicht.	Selektiv – Offen für ausländische Tools innerhalb von Grenzen; zielt darauf ab, Abhängigkeiten zu reduzieren und gleichzeitig EU-ausgerichtete internationale Engagements zu unterstützen.	Investitionsorientiert
Dänemark	Hoch – Substantial Investitionen in dänische LLMs, nationale Rechenkapazitäten und offene Sprachdaten.	Hoch – Strebt an, dass KI die dänische Sprache und Kultur widerspiegelt; implementiert EU-konforme Schutzmaßnahmen.	Sehr hoch – Menschzentrierte Governance, KI-Arbeitsgruppe und beratende Unterstützung sind in die nationale Strategie integriert.	Selektiv – Nutzt ausländische Tools, priorisiert jedoch souveräne Entwicklungen für linguistisch und ethisch kritische Anwendungsfälle.	Investitionsorientiert
Deutschland	Hoch – Bedeutende Investitionen in KI-Infrastruktur, Forschung & Entwicklung, Hochleistungsrechnen und Talentförderung; Fokus auf die Entwicklung vertrauenswürdiger, einheimischer KI-Systeme.	Hoch – Betont technologische Souveränität und KI-Sicherheit mit strengen Kontrollen beim Einsatz externer KI-Modelle, einschließlich Datenschutz, Transparenz und Sicherheit.	Hoch – Starkes Governance-Rahmenwerk mit verantwortlichen Personen für KI, klaren Richtlinien zur ethischen Nutzung von KI und rigorosen Tests zur KI-Integration, wobei die Umsetzung noch in der Entwicklung ist.	Selektiv – Bereitschaft zur Nutzung ausländischer LLMs unter strengen Sicherheits-, Datenschutz- und vertraglichen Bedingungen, mit Betonung auf nationaler Kontrolle und Datensouveränität.	Investitionsorientiert
Estland	Hoch – Finanzierung nationaler Cloud- und estnischer Sprachtechnologie, Teilnahme an EuroHPC und Förderung der Wiederverwendung von Open Source.	Hoch – Rechtliche und ethische Schutzmaßnahmen konzentrieren sich auf Vertrauen, Privatsphäre und die Einhaltung von EU-Rahmenbedingungen.	Sehr hoch – Starke Aufsicht mit Transparenzstandards, rechtlicher Beteiligung und Programmen zur KI-Bildung.	Selektiv – Offen für internationale Kooperationen, behält jedoch den Fokus auf nationaler Relevanz und Kontrolle.	Investitionsorientiert
Finnland	Mäßig bis hoch – Investiert in finnische Sprachmodelle (z. B. Finnish GPT, Poro) und nationale Open-Source-Plattformen, obwohl die Marktgrößenbeschränkungen erkannt werden.	Hoch – Besorgt über die Dominanz ausländischer Technologien; priorisiert Autonomie, insbesondere in sprachlich sensiblen Bereichen.	Hoch – Risikobewertungen und gesellschaftliche Aufsicht werden betont; hält sich an den AI-Act mit praktischen Governance-Tools wie dem Responsible AI Canvas.	Hoch – Weitgehende Übernahme kommerzieller LLMs (z. B. über Microsoft, IBM), während Risiken verwaltet und in öffentliche Dienste integriert werden.	Balanciert

Land	Investitionen in digitale Souveränität bei KI und LLMs	Digitale Souveränität & Risikobewusstsein	Governance & menschliche Kontrolle	Offenheit gegenüber ausländischen LLMs	Archetyp
Frankreich	Hoch – Großangelegte öffentliche Investitionen in KI-F&E, französisch spezifische Modelle und souveräne Infrastruktur durch Initiativen wie INESIA und ALT-EDIC.	Hoch – Starke Betonung auf Datenkontrolle, strategischer Autonomie und der Auswahl von Abhängigkeiten anstelle von vollständiger Vermeidung.	Hoch – Umfassende ethische Prinzipien, Aufsichtsräume und CNIL als vorgeschlagener KI-Regulator; starke Ausrichtung auf den AI-Act	Mäßig – Nutzt ausländische LLMs in kontrollierten Szenarien, bevorzugt jedoch EU-Anbieter für sensible Anwendungen.	Balanciert
Irland	Niedrig bis mäßig – Fokussiert sich auf die Entwicklung des Ökosystems und die Teilnahme an EU-Programmen; begrenzte Betonung auf die Entwicklung souveräner Modelle.	Mäßig – Starke Datenschutzorientierung, aber es fehlen detaillierte Strategien zur rechtlichen Reichweite oder zur Vermeidung von Anbieter-Lock-in.	Hoch – Wendet die Prinzipien der EU zur vertrauenswürdigen KI an und bewertet Risiken, mit Fahrplänen und Governance-Tools wie dem Responsible AI Canvas.	Hoch – Fördert die Übernahme ausländischer LLMs in den öffentlichen Dienst und betont Vorteile bei gleichzeitiger Verwaltung von Datenschutz und Sicherheit.	Pragmatisch
Italien	Hoch – Entwicklung italienischer LLMs und nationaler KI-Plattformen; große Investitionen in Talente und Infrastruktur (z. B. PhD-AI.it, LMMs).	Hoch – Stellt ausländische LLMs als kulturell nicht abgestimmt und strategisches Risiko dar; betont maßgeschneiderte nationale Entwicklung.	Hoch – Ethikkommissionen, Datensatzregister und die Einhaltung der EU-Vorschriften gewährleisten starke Aufsicht und Transparenz.	Niedrig – Drückt klare Zurückhaltung aus, sich auf ausländische LLMs zu verlassen; Übernahme ist begrenzt und vorsichtig.	Konservativ
Japan	Mäßig – Konzentriert sich auf KI-Sicherheitsinfrastruktur, Fähigkeiten und Governance; bislang keine klare nationale LLM-Entwicklung.	Hoch – Risikobewusst, insbesondere im Hinblick auf Fehlinformationen, geistiges Eigentum und grenzüberschreitende Datenexposition; betont rechtliche Compliance für ausländische Akteure.	Hoch – Menschzentrierter Ansatz mit Input von mehreren Interessengruppen; umfasst CAIO-Rollen, Beratungsräte und Risikoverifizierung.	Hoch – Stimmt mit globaler KI-Governance überein und fördert eine sichere Nutzung durch internationale Zusammenarbeit, anstatt Einschränkungen vorzunehmen.	Balanciert
Kanada	Niedrig – Keine bedeutende Investition in souveräne LLMs oder Infrastruktur; Strategie konzentriert sich auf Politik und Richtlinien.	Hoch – Regierung warnt davor, öffentliche LLMs für sensible Daten zu verwenden, und betont starke Daten-Governance.	Sehr hoch – Robuste Aufsicht durch obligatorische algorithmische Auswirkungen, Transparenzvorschriften und öffentliche Register.	Hoch – Fördert aktiv die sorgfältige Nutzung ausländischer LLMs; der Fokus liegt auf Risikomanagement, nicht auf nationaler Herkunft.	Pragmatisch
Malaysia	Hoch – Positioniert sich als Innovator mit Investitionen in F&E, KI-Hubs, Bildung und öffentlich-private Partnerschaften zur Entwicklung nationaler Fähigkeiten.	Mäßig bis hoch – Betonung des KI-Risikomanagements, Cybersecurity und sicherer Implementierung, obwohl einige Rahmenbedingungen noch in der Entwicklung sind.	Hoch – Fördert inklusive, ethikbasierte KI-Governance mit Partnerschaften aus mehreren Sektoren und verantwortungsvollen Innovationsrahmen.	Hoch – Offen für ausländische Kooperation und KI-Übernahme; zielt darauf ab, das globale Profil zu stärken und externes Fachwissen zu nutzen.	Investitionsorientiert
Niederlande	Hoch – Bedeutende Investitionen in nationale KI (z. B. GPT-NL-Projekt, nationale Supercomputing) und Entwicklung hauseigener Expertise.	Hoch – Geht aktiv Risiken einer ausländischen Abhängigkeit an; unterstützt »strategische digitale Autonomie« und nationale Resilienz.	Hoch – Betont Transparenz, Erklärbarkeit und öffentliche Verantwortlichkeit durch EU-konforme, menschzentrierte Politik.	Hoch – Begrüßt ausländische Innovation, insbesondere innerhalb der EU-Rahmen, während nationale Schutzvorkehrungen beibehalten werden.	Balanciert

Land	Investitionen in digitale Souveränität bei KI und LLMs	Digitale Souveränität & Risikobewusstsein	Governance & menschliche Kontrolle	Offenheit gegenüber ausländischen LLMs	Archetyp
Norwegen	Hoch – Investiert in Sprachressourcen und spezialisierte nationale Infrastruktur, mit Plänen für weit verbreitete KI-Nutzung in der Regierung.	Hoch – Priorisiert Privatsphäre und Cybersicherheit, erkundet regulatorische Werkzeuge und fördert Daten-Governance.	Hoch – Menschzentrierter, transparenter und ethikgeführter Ansatz; Koordination und Kompetenzentwicklung sind entscheidend.	Hoch – Nimmt an EU- und internationalen Kooperationen teil; zielt darauf ab, von globaler KI zu profitieren und gleichzeitig starke lokale Kontrollen aufrechtzuerhalten.	Balanciert
Österreich	Hoch – Bedeutende Mittel für KI-F&E, Pläne für nationale GPU-Cluster und Unterstützung souveräner Infrastruktur.	Hoch – Eindeutiges Ziel, Abhängigkeit von globalen Monopolen zu vermeiden; Priorität auf Privatsphäre, Datenschutz und europäischen Datenräumen.	Sehr hoch – Menschzentrierte Strategie mit vorgeschriebener Aufsicht, partizipativer Gestaltung und regulatorischer Erkundung.	Selektiv – Kooperativ innerhalb der EU-Rahmenbedingungen, aber widerstandsfähig gegenüber unkontrollierter Übernahme externer Modelle; Souveränität betont.	Konservativ
Saudi-Arabien	Hoch – Bedeutende Investitionen über SDAIA in nationale KI-Infrastruktur, Forschung und Arbeitskräfte, um das Land als globalen KI-Hub zu positionieren.	Hoch – Klare Regeln zur Untersagung von KI mit inakzeptablem Risiko (z. B. Profiling), mit starken nationalen Kontrollen über Daten und KI-Nutzung.	Stark – Vorgeschriebene Aufsicht, ethische Prinzipien und zentrale Governance durch SDAIA für die Lebenszyklussteuerung von KI-Systemen.	Selektiv – Offen für ausländische Partnerschaften, balanciert diese jedoch vorsichtig mit nationaler Kontrolle und souveränen Prioritäten.	Offensiv
Schweden	Mäßig – Fokussiert sich auf Forschung und Talententwicklung von Weltklasse, unterstützt von großen Stiftungen und nationalem »high-performing-computing«.	Hoch – Betont ethikbasiertes KI-Design, GDPR-Compliance und proaktive Risikowahrnehmung in der Systemgestaltung.	Stark – Fördert nachhaltige, menschlich geprüfte KI-Systeme mit Transparenz, ethischen Standards und Verantwortung in öffentlichen Diensten.	Offen – Engagiert sich global, insbesondere innerhalb der EU, und erkennt die Bedeutung internationaler KI-Zusammenarbeit und Innovation an.	Balanciert
Singapur	Hoch – Substantielles Funding für nationale KI-Programme, nationale Rechenleistung und Talent über Initiativen wie AI Singapore.	Hoch – Bekannt für proaktive Risikogovernance, einschließlich Tools wie AI Verify und dem Model AI Governance Framework.	Stark – Menschzentrierte Prinzipien (FEAT), ethische Aufsichtsorgane und strukturierte Risikogovernance gewährleisten hohe Reife.	Höchst offen – Begrüßt ausländische Firmen und Forscher:innen und positioniert sich als internationales KI-Testfeld und Standardschaffer.	Offensiv
Südkorea	Hoch – Großangelegte Investitionen in KI-Chips, Infrastruktur (KI-Hub) und Innovationscluster zur Förderung souveräner KI-Technologie.	Hoch – Risikobewusste regulatorische Reformen (z. B. überarbeitete Datenschutzgesetze), die Probleme wie Deepfakes und systemische Schwächen angehen.	Stark – Ethikrichtlinien für KI, Schutz der Menschenrechte und Governance-Mechanismen für hochwirksame Systeme.	Vorsichtig – Bevorzugt die Entwicklung nationaler LLMs und technologische Führerschaft, ist jedoch offen für strategische internationale Zusammenarbeit.	Investitionsorientiert
Taiwan	Hoch – Der KI-Aktionsplan 2.0 finanziert F&E, Talent, inländische Chips und Software; betont den Aufbau einheimischer Fähigkeiten.	Hoch – Das KI-Grundgesetz adressiert nationale Sicherheitsrisiken durch ausländische KI und betont Vorurteile, Hintertüren und Resilienz.	In Entwicklung – Entwurf einer Governance-Struktur, die sich am AI-Act orientiert; ethische Richtlinien existieren, aber Durchsetzung und Rollen sind noch in der Verfeinerung.	Offen – Begrüßt ausländische Investitionen und Cloud-Infrastruktur, während vorsichtig regulatorische ursprungsbezogene Einschränkungen erkundet werden.	Investitionsorientiert

Land	Investitionen in digitale Souveränität bei KI und LLMs	Digitale Souveränität & Risikobewusstsein	Governance & menschliche Kontrolle	Offenheit gegenüber ausländischen LLMs	Archetyp
UK	Mäßig bis hoch – Bedeutende Mittel in F&E und KI-Talente; erkennt Rechenbeschränkungen an; zielt auf den Status einer KI-Supermacht ab.	Hoch – Adressiert sowohl kurz- als auch langfristige KI-Bedrohungen (Deepfakes, AGI); führt Risikobewertungen von Lieferketten und Grundmodellen durch.	Stark – Verpflichtet zu Transparenzstandards, Human-in-the-loop und öffentlichen Registern; setzt ethische KI-Nutzung im öffentlichen Sektor durch.	Offen – Arbeitet international an F&E und Standards, während regulatorische Unabhängigkeit und inländische Innovation aufrechterhalten werden.	Balanciert
VAE	Hoch – Starke Investitionen in KI-Institute, Beschleuniger und Transformation des öffentlichen Sektors; zielt darauf ab, globaler KI-Führer zu werden.	Hoch – Klassifiziert GenAI-Risiken; verbietet kritische Entscheidungen durch KI; bettet Privatsphäre und nationale Ausrichtung in Richtlinien ein.	Stark – Ethikbasierter Ansatz mit Menschenzentriertheit, Überprüfung von GenAI-Ergebnissen und Governance-Organen wie dem KI-Rat.	Höchst offen – Zieht aktiv ausländische Firmen und Talente an, um die nationale Kapazität durch internationale Kooperation zu beschleunigen.	Offensiv

A.5 Indikatoren

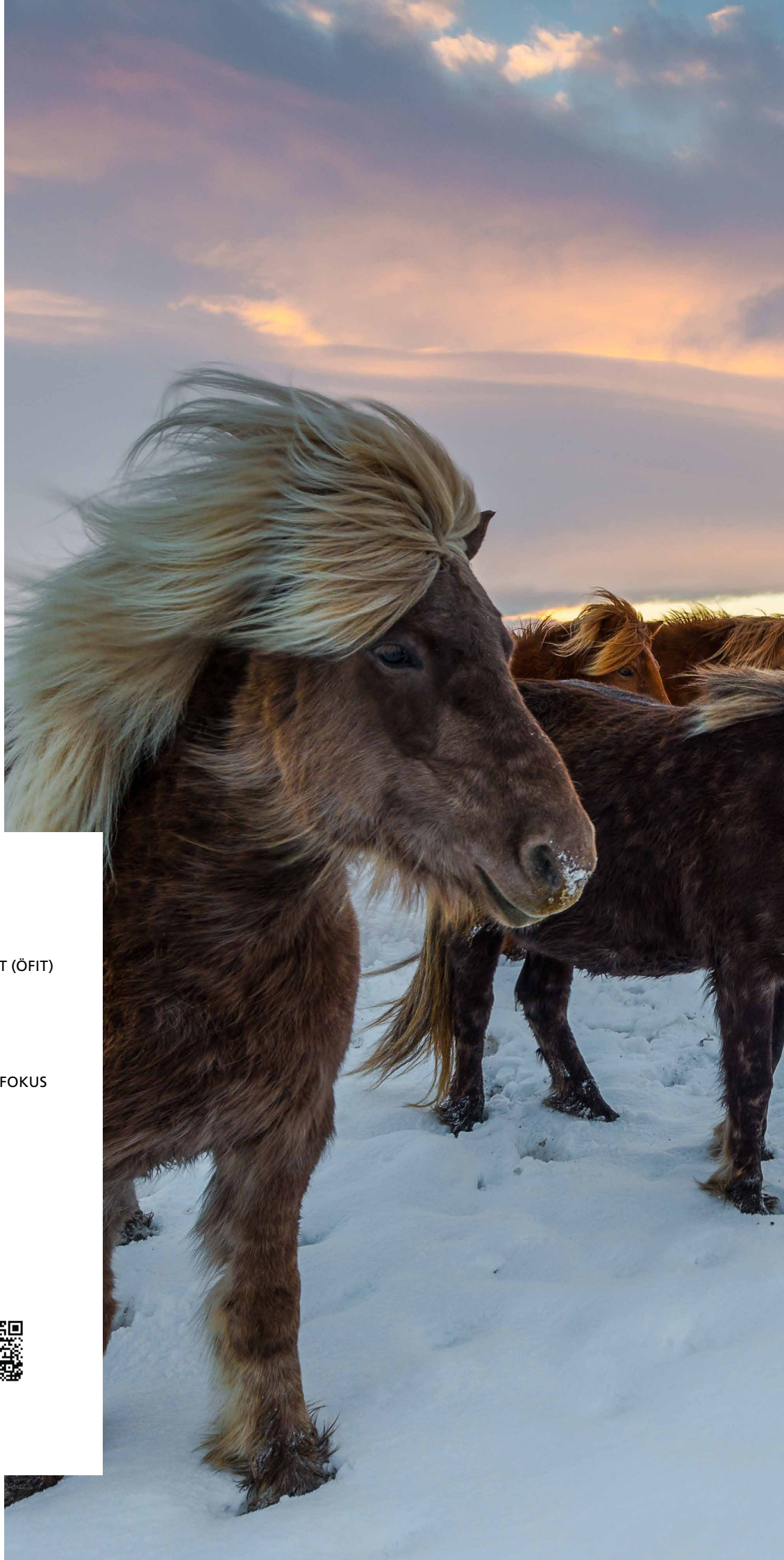
Wechselmöglichkeit	Beschreibung	Ausprägungen
Modularität	einzelne Komponenten / Funktionen können ohne eine Anpassung der Gesamtarchitektur ausgetauscht werden	0: Kaum möglich 1: Weniger einfach 2: Einfach 3: Sehr einfach
Nachnutzbarkeit	Die Anwendung wird (zentral) bereitgestellt, sodass andere sie nutzen können	0: Nein 3: Ja, z.B. Open Source
Open Source	Der Programmcode der Anwendung bzw. des Modells steht als OSS zur Verfügung	0: Nein 2: Nein, aber geplant 3: Ja
Anzahl alternativer Modelle	Qualitativ ernst zu nehmende Alternativen zur gewählten Lösung wurden getestet	0: Nein 2: Eine Alternative getestet 3: Mehrere Alternativen getestet
Flexible Modellwahl	Innerhalb der Anwendung lässt sich flexibel zwischen LLMs (verschiedener Anbieter) wechseln	0: Nein 1: Ja, innerhalb eines Anbieters 3: Ja, zwischen verschiedenen Anbietern
Cloud vs. On-Premise	Anwendung und Modell laufen auf Hardware, die einen Wechsel ermöglicht	0 : Public Cloud 3: Eigener Betrieb oder öffentlicher IT-DL
Dateiformate	Standardisierte und nicht-proprietäre Dateiformate erleichtern den Wechsel zwischen funktional ähnlichen Systemen	0: liegen nicht standardkonform vor 1: liegen teilweise vor 3: liegen vollständig vor

Gestaltungsfähigkeit	Beschreibung	Ausprägungen
Softwaredokumentation	Die Anwendung verfügt über eine umfassende, strukturierte und aktuelle Dokumentation zur Nutzung	0: keine Dokumentation 1: wenig ausführlich 2: ausführlich 3: sehr ausführlich
Technische Kompetenzen	Es sind technische Kompetenzen innerhalb des Teams vorhanden	0: keine Kompetenzen (<3 Punkte) 2: mittlere Kompetenzausprägung (3-7 Punkte) 3: Starke Kompetenzausprägung (7-10 Punkte)
Austausch und gegenseitiges Lernen	Es findet ein Erfahrungsaustausch mit anderen KI-Projekten statt (z. B. in Arbeitsgruppen, Fachkonferenzen, digitalen Angeboten)	0: Nein 3: Ja, z.B. Arbeitsgruppen, Konferenzen Plattformen
Informationsbereitstellung	Es existiert eine ausführliche Informationsbereitstellung des LLM-Anbieters zum Modell	0: keine Informationen 1: wenig ausführlich 2: ausführlich 3: Sehr ausführlich
Open-Source-Modell	Das LLM ist in Teilen oder vollständig Open Source, siehe auch 3.2	0: Nein 2: Ja, teilweise 3: Ja, vollständig
Zusammenarbeitsstrukturen	Es existieren Strukturen, die eine Zusammenarbeit mit Bezug auf die technische Infrastruktur ermöglichen (zum Beispiel geteilte Rechenkapazitäten)	0: Nein 3: Ja
Datenquellen & Verfügbarkeit	Die verwendeten Daten sind frei verfügbar, eigene Daten oder von einem kommerziellen Anbieter	Eigene Daten Öffentlich, frei verfügbare Daten Kommerzielle Daten
Datenanpassbarkeit	Es gibt Strukturen, die Datenmanagement ermöglichen	0: sehr hoher Aufwand 1: mittlerer Aufwand 2: geringer Aufwand 3: nahezu kein Aufwand

Einfluss auf Anbieter	Beschreibung	Ausprägungen
Geschlossene Ökosysteme	Wenn Anwendungen Teil eines proprietären (geschlossenen) Ökosystems sind besteht die Gefahr eines Vendor-Lock Ins	0: Ja, Anwendung ist Teil davon 3: Nein, Anwendung läuft unabhängig
Rechtliche Kompetenzen	Kompetenzen zu Ethik, Recht und Normen innerhalb des Projektteams sind Voraussetzung, um Bedarfe und Anforderungen der öV in Vertragsverhandlungen mit Anbietern artikulieren und durchsetzen zu können	0: keine Kompetenzen (<3 Punkte) 2: mittlere Kompetenzausprägung (3-7 Punkte) 3: Starke Kompetenzausprägung (7-10 Punkte)
Zertifizierungen	Es liegen Zertifikate des Anbieters hinsichtlich digitaler Souveränität vor. Nur relevant falls kein Selbstbetrieb	0: Nein 2: Geplant 3: Ja
Sitz des Anbieters	Der Anbieter von Anwendung und Modell hat seinen Hauptstandort in Europa. Nur relevant falls kein Selbstbetrieb	0: Nein 3: Ja
Standort/Anbieter der Cloudserver	Die Server von Anwendung und LLM stehen in Europa	0: Nein 3: Ja

A.6 Ergebnisse entlang der Indikatoren

Wechselmöglichkeit	**44,7%**	**Gestaltungsfähigkeit**	**62,09%**	**Einfluss auf Anbieter**	**47,71%**
Modularität	**61%**	Softwaredokumentation	**66%**	Geschlossene Ökosysteme	**75%**
Nachnutzbarkeit	**24%**	Technische Kompetenzen	**71%**	Rechtliche Kompetenzen	**37%**
Open Source	**35%**	Austausch und gegenseitiges Lernen	**61%**	Zertifizierungen	**24%**
Anzahl alternativer Modelle	**26%**	Informationsbereitstellung	**38%**	Verhandlungsmacht	**83%**
Flexible Modellwahl	**52%**	Open-Source-Modell	**35%**	Sitz des Anbieters	**21%**
Cloud vs. On-Premise	**68%**	Zusammenarbeitsstrukturen	**61%**	Standort/Anbieter der Cloudserver	**100%**
Dateiformate	**41%**	Datenquellen & Verfügbarkeit	**66%**		
Cloud LLM:	**44%**	Datenanpassbarkeit	**50%**		



Kontakt

Dorian Wachsmann
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de

linkedin.com/company/oefit

ISBN: 978-3-948582-33-3

11|25