

Kritische Analyse des UK–OpenAI MoU (Juli 2025): Langfristige Implikationen für KI-Infrastruktur und öffentlichen Sektor

Kurzfassung der wichtigsten Erkenntnisse (Executive Summary)

- **Partnerschaft ohne Rechtsbindung:** Das im Juli 2025 geschlossene Memorandum of Understanding (MoU) zwischen dem britischen Department for Science, Innovation & Technology (DSIT) und OpenAI ist **freiwillig und rechtlich unverbindlich**, wodurch klare Verpflichtungen fehlen[1]. Diese Unverbindlichkeit wirft Fragen zur **Durchsetzbarkeit** auf – etwa was passiert, wenn Zusagen unerfüllt bleiben, da **Sanktions- oder Streitbelegungsmechanismen** im MoU nicht vorgesehen sind.
- **Datenhoheit und Transparenzrisiken:** Kritiker warnen, die Vereinbarung sei „hoffnungslos vage“ in ihren Details[2]. Unklar bleibt, **welche öffentlichen Daten** OpenAI nutzen darf und ob britische Bürgerdaten unter **UK-Datenschutz** verbleiben. Angesichts der US-Gesetze (CLOUD Act, FISA 702), die **extraterritorialen Zugriff** auf Daten US-amerikanischer Firmen erlauben[3][4], droht ein Konflikt mit britisch/europäischem Datenschutz. Eine Parlamentsausschuss-Vorsitzende verglich das Abkommen mit dem „**Fuchs im Hühnerstall**“, da OpenAI potentiell enorme Vorteile aus staatlichen Daten ziehen könnte[5].
- **Technologische Abhängigkeit:** Die Kooperation birgt die Gefahr eines **Vendor Lock-in**. OpenAI’s proprietäre KI-Modelle könnten essenziell für britische Systeme werden, was **Exit-Strategien** erschwert. Bereits jetzt sind OpenAI-Technologien (z.B. GPT-4 basierter Assistent „Humphrey“) im britischen Staatsdienst im Einsatz[6]. Ohne Diversifizierung besteht ein **Resilienz-Problem**: Änderungen der OpenAI-Strategie, Preismodell oder technische Ausfälle könnten **kritische Dienste** beeinträchtigen. Die **Reversibilität** der Integration – also ein späterer Wechsel auf alternative (z.B. Open-Source) Lösungen – wäre technisch und finanziell aufwändig.
- **Wirtschaftliche und wettbewerbliche Folgen:** Die Regierung verspricht sich **£47 Mrd. jährliches BIP-Wachstum und +1,5 % Produktivität** durch KI[7][8], doch ob OpenAI diese Erwartungen erfüllt, bleibt unsicher. Es besteht das Risiko einer **Marktverzerrung** zulasten heimischer KI-Startups: Eine privilegierte Partnerschaft

mit OpenAI könnte lokale Innovatoren verdrängen. Zudem sind viele Zusagen **unverbindliche Absichtserklärungen** („OpenAI *könnte* investieren...“)[9], sodass die Diskrepanz zwischen angekündigten Investitionen und **tatsächlicher Wirkung** kritisch beobachtet werden muss. **Lock-in-Effekte** durch proprietäre APIs und geschlossene Standards könnten die öffentliche Hand langfristig an einen US-Anbieter binden und **Folgekosten** erhöhen. Automatisierungspotenziale (z.B. bei Verwaltungsaufgaben) könnten zwar Effizienz steigern, aber auch **Arbeitsplätze im öffentlichen Sektor** einsparen – mit sozialen Implikationen.

- **Demokratisch-gesellschaftliche Dimension:** Die Einführung von **KI-Entscheidungssystemen in Justiz, Verwaltung oder Sicherheitsapparat** ohne ausreichende demokratische Kontrolle birgt erhebliche Gefahren. Proprietäre Modelle wie GPT-4 sind **Black Boxes**, was **Transparenz und Rechenschaftspflicht** erschwert. Bisherige Erfahrungen zeigen, dass algorithmische Lösungen etwa im Justizwesen **Bias und Fehler** aufweisen können[10]. Ohne **öffentliche Debatte** und Einbindung aller Stakeholder (z.B. Justiz, Zivilgesellschaft) droht **Akzeptanzverlust** in der Bevölkerung. Bereits jetzt werden mangelnde Transparenz und fehlende parlamentarische **Konsultation** kritisiert[11][12].
- **Geopolitische Positionierung:** Die Kooperation positioniert Großbritannien als **Sprungbrett** für OpenAI nach Europa (post-Brexit) und spiegelt die enge **UK-USA-Tech-Allianz** wider[13]. Durch die Einbindung US-amerikanischer Big-Tech-Firmen in kritische Infrastruktur gibt das UK de facto ein Stück **digitale Souveränität** auf, trotz rhetorischer Beteuerungen von „Sovereign AI“[14][15]. Im Vergleich zur **EU-Strategie (AI Act)**, die stärker regulierend und auf **Risikominimierung** ausgerichtet ist, verfolgt das UK einen industrie-freundlicheren Kurs, ähnlich der **US-Linie ohne umfassende KI-Regulierung**[16]. Dies könnte Vorteile bei Investments bringen, aber auch Spannungen mit EU-Partnern erhöhen. Historisch erinnert die Lage an frühere **Technologie-Abhängigkeiten** (z.B. britische Abhängigkeit von US-Tech bei Cloud, Betriebssystemen oder früher in Telekommunikation), die langfristig politische und wirtschaftliche Nachteile mit sich brachten.

Kernfrage: Wie kann das Vereinigte Königreich die Vorteile von KI-Innovationen nutzen, ohne seine **digitale Souveränität** und **demokratische Kontrolle** zu verlieren? – Im Folgenden werden die einzelnen Dimensionen der Partnerschaft analysiert, versteckte Risiken offengelegt und Handlungsalternativen aufgezeigt, um einen **ausgewogenen Kurs** zwischen Innovationsförderung und Souveränitätsschutz zu finden.

1. Einleitung und Kontext

Die britische Regierung (DSIT) und OpenAI unterzeichneten am 21. Juli 2025 ein Memorandum of Understanding, um eine strategische Zusammenarbeit im Bereich **künstliche Intelligenz (KI)** zu starten[17]. Dieses MoU wird von beiden Seiten als Meilenstein dargestellt, um die **digitale Transformation** des öffentlichen Sektors zu beschleunigen und Großbritanniens Stellung als führende KI-Nation zu festigen[18][19].

Inhaltlich skizziert das MoU drei Hauptfelder der Kooperation[20]:

- **KI-Infrastruktur aufbauen:** OpenAI soll bei der Entwicklung von KI-Infrastruktur in UK helfen, u.a. durch mögliche **Investitionen in Rechenzentren** („AI Growth Zones“)[21]. Die Regierung hat hierfür bereits £2 Mrd. Fördermittel bereitgestellt und über 200 Standortvorschläge erhalten[22].
- **Einsatz von OpenAI-Modellen im öffentlichen Dienst:** OpenAI's Modelle (z.B. GPT-4) sollen in Ministerien und Behörden getestet werden, um **Verwaltungsabläufe zu optimieren** (z.B. Analyse von Bürgerfeedback durch den Humphrey-KI-Assistenten)[6]. Geplant ist der schrittweise Einsatz in sicherheitskritischen Bereichen wie **Justiz, Verteidigung, Bildung**[23].
- **KI-Sicherheit und Forschung:** Eine engere Kooperation mit dem neuen **UK AI Safety/Security Institute** soll Wissenstransfer ermöglichen, insbesondere hinsichtlich **Modellfähigkeiten und Risiken** fortgeschrittener KI[24]. Geplant ist ein technisches Informationsaustausch-Programm, um gemeinsam **Schutzmaßnahmen** zu entwickeln[24].

Das MoU wird ausdrücklich als **freiwillig und „nicht rechtsverbindlich“** bezeichnet[1]. Finanzielle Verpflichtungen sind nicht festgeschrieben – es fließt zunächst **kein öffentliches Geld**, und OpenAI erhält im Gegenzug vorerst keinen exklusiven Beschaffungsvertrag[25]. Stattdessen handelt es sich um eine **Absichtserklärung** mit vielen Prüfaufträgen („explore...“, „könnte...“)[9]. Die britische Regierung feierte die Vereinbarung dennoch als großen Erfolg auf dem Weg zur „AI Superpower“[26][27]. Premierminister Keir Starmer hatte die Förderung von KI als Teil seines **AI Opportunities Action Plan** (Januar 2025) priorisiert, um die schwächelnde Wirtschaft anzukurbeln[18][8].

Problemaufriss: Trotz der ambitionierten Ziele wirft das MoU eine Reihe **kritischer Fragen** auf. Schon kurz nach Bekanntwerden forderten Abgeordnete und Experten **Transparenz** über die Inhalte des Deals[28][12]. Die Vereinbarung wurde ohne öffentliche Ausschreibung oder breiten Stakeholder-Dialog geschlossen – offenbar begünstigt durch

persönliche Kontakte des Tech-Ministers zu OpenAI und Google[29]. Befürchtet werden **ungleiche Machtverhältnisse**, in denen eine US-Firma Einfluss auf britische Staatsaufgaben gewinnt, **ohne demokratische Legitimation oder Haftung**. Dieses Papier untersucht systematisch die langfristigen Implikationen der Partnerschaft in sechs Dimensionen (rechtlich, datenschutzrechtlich, technologisch, ökonomisch, gesellschaftlich, geopolitisch). Durch eine **wissenschaftlich fundierte** Analyse sollen versteckte Risiken und Pfadabhängigkeiten aufgezeigt werden – mit dem Ziel, **Handlungsempfehlungen** zu formulieren, wie das UK Innovation und Souveränität ausbalancieren kann.

2. Methodik und analytischer Rahmen

Für die vorliegende Untersuchung wurde ein **mehrdimensionaler Analyseansatz** gewählt, der sowohl juristische/politische Aspekte als auch technische und ökonomische Faktoren berücksichtigt:

- **Literatur- und Quellenrecherche:** Grundlage ist die Auswertung primärer Dokumente (Originaltext des MoU[30], der **AI Opportunities Action Plan**, relevante DSIT-Strategiepapiere) sowie sekundärer Quellen (Presseberichte, Tech-Policy-Analysen, parlamentarische Debattenbeiträge). Insbesondere wurden aktuelle **Peer-Review-Studien** zur KI-Governance und **Positionspapiere** von zivilgesellschaftlichen Organisationen (z.B. Ada Lovelace Institute, Foxglove) herangezogen, um unabhängige Perspektiven einzubeziehen. Alle Fakten werden mit **verlässlichen Quellen** nachgewiesen; bei Unsicherheiten wird dies transparent gemacht.
- **Stakeholder-Mapping:** Identifikation der **beteiligten Akteure** und Interessen. Dazu zählen die britische Regierung (DSIT, weitere Ministerien wie Verteidigung oder Justiz), OpenAI als Unternehmen, **britische KI-Startups und Tech-Industrie**, die Zivilgesellschaft (Bürgerrechtsorganisationen, Datenschützer) sowie internationale Akteure (EU, USA, Konkurrenten wie Google/Anthropic). Mögliche **Interessenkonflikte** – etwa die Doppelfunktion Peter Kyles als Förderer und Kontrolleur von Big Tech – werden benannt.
- **SWOT-Analyse (Stärken/Schwächen/Risiken/Chancen):** Fokussiert auf Abhängigkeitsfragen und Souveränitätsaspekte. Hierbei werden die **kurzfristigen Vorteile** (z.B. Know-how-Transfer, Investitionen, Effizienzgewinne) den **langfristigen Risiken** (Lock-In, Machtasymmetrien) gegenübergestellt.

- **Pfadabhängigkeitsanalyse:** Untersuchung, inwiefern frühe Entscheidungen (z.B. Wahl eines proprietären OpenAI-Ökosystems) die **zukünftigen Handlungsoptionen** des UK einschränken. Dies umfasst die Analyse der **Reversibilität** der Integration und welche **Exit-Strategien** (Wechsel des Anbieters, Aufbauen einer eigenen KI) realistisch umsetzbar wären, falls die Partnerschaft scheitert oder unerwünschte Wirkungen zeigt.
- **Vergleichende Policy-Analyse:** Gegenüberstellung mit ähnlichen Fällen international. Betrachtet werden z.B. die **EU KI-Regulierung (AI Act)** versus die UK-Vorgehensweise, **US-UK Tech-Kooperationen** (z.B. Google Cloud MoU)[31][32], sowie Ansätze anderer Länder (z.B. Frankreichs Fokus auf europäische „Souveräne KI“, Chinas staatlich gesteuerte KI-Programme). Auch historische Parallelen technischer Abhängigkeit (z.B. bei Cloud-Anbietern oder früher beim 5G-Netzausbau mit Huawei) fließen ein.
- **Risikobewertung:** Entwicklung einer **Risikomatrix**, die zentrale Risikofelder identifiziert (Datenabfluss, Regulierungsabhängigkeit, Marktverzerrung, technisches Versagen, etc.). Für jedes Risiko werden **Wahrscheinlichkeit** und **Auswirkungsgrad** qualitativ (hoch/mittel/niedrig) eingeschätzt und gegenübergestellt. Konfidenzintervalle in den Bewertungen werden angegeben, um verbleibende Unsicherheiten kenntlich zu machen.
- **Szenario-Analyse (Zeithorizont 2025–2035):** Basierend auf den Forschungsergebnissen werden drei plausible **Zukünfte** entworfen – von einer Worst-Case-Dystopie bis zu einem Best-Case-Szenario – inklusive der Eintrittswahrscheinlichkeiten. Diese Szenarien („OpenAI-Hegemonie“, „Multilaterale Balance“, „Technologische Fragmentierung“) dienen dazu, die Bandbreite der möglichen Entwicklungen aufzuzeigen und **Frühindikatoren** für deren Eintritt abzuleiten.

Die Kombination dieser Methoden gewährleistet eine **ganzheitliche, evidenzbasierte Betrachtung**. Fakten und Analyse werden klar getrennt präsentiert: Zunächst erfolgt die Darstellung der Befunde in den Kapiteln 3–8 entlang der vorgegebenen Dimensionen, gefolgt von der übergreifenden Diskussion (Kap. 9) der **kritischen Leitfragen**. Abschließend werden in Kap. 10 konkrete **Handlungsempfehlungen** für Politik und Verwaltung formuliert, die als **Policy-Brief** dienen können. Der Bericht erfüllt wissenschaftliche Qualitätsstandards (APA 7 konforme Zitation, Transparenz zu Unsicherheiten) und soll Entscheidungsträgern pragmatische Optionen an die Hand geben, um die **digitale Souveränität** Großbritanniens trotz KI-Kooperation mit einem US-Konzern zu wahren.

3. Rechtliche und Governance-Analyse

In diesem Abschnitt werden die **rechtlichen Rahmenbedingungen** und Governance-Aspekte des MoU beleuchtet: Welche Implikationen hat die rechtliche Unverbindlichkeit? Wie werden Haftungsfragen und Konfliktlösung geregelt (oder eben nicht)? Gibt es institutionelle Kontrollmechanismen? Zudem wird der **Entscheidungsprozess** hinter dem MoU kritisch betrachtet (Stichwort Transparenz, Ausschreibung, Interessenkonflikte).

3.1 Unverbindlichkeit und fehlende Durchsetzung

Das MoU ist ausdrücklich als „**voluntary, not legally binding**“ deklariert[1]. Diese rechtliche Unverbindlichkeit bedeutet:

- **Keine einklagbaren Pflichten:** Weder OpenAI noch die britische Regierung sind durch das MoU zu konkreten Leistungen verpflichtet. Formulierungen wie „*explore*“ (erkunden) tauchen mehrfach auf (laut Analyse sechsmal im Text)[9], was den **Absichtscharakter** betont. So heißt es etwa, OpenAI "*könnte* in AI Growth Zones investieren"[9] – eine unverbindliche Absicht ohne Garantien. Im Kern hat der Tech-Minister mit OpenAI **keinen belastbaren Vertrag** ausgehandelt, was ein Branchenkommentator spöttisch als "*legally meaningless love-in*" bezeichnete[33].
- **Keine Sanktionsmechanismen:** Weil keine rechtlich bindenden Zusagen existieren, fehlen auch **Durchsetzungs- und Sanktionsmechanismen**. Sollte OpenAI z.B. zugesagte Investitionen nicht tätigen oder Qualitätsstandards nicht einhalten, hätte die Regierung **keinen vertraglichen Hebel**, um dies einzufordern. Dies ist ein wesentliches Governance-Problem: Die Umsetzung hängt vom *Goodwill* und den Geschäftsinteressen OpenAIs ab. Kritiker bemerken, dass das UK hier **viel Vertrauen vorschießt**, ohne Absicherung im Streitfall[34].
- **Keine Streitbeilegungsregelung:** Übliche Regierungsverträge enthalten Klauseln, wie Differenzen gelöst werden (Mediationen, Gerichtsstand etc.). Im MoU fehlen solche Regelungen vollständig. Sollte es zu **Konflikten** kommen – etwa bezüglich Datenzugang oder Leistungserbringung – gibt es **keinen definierten Prozess** zur Klärung. Die Parteien müssten neu verhandeln oder das MoU jederzeit einseitig aufkündigen, da es nur politisch bindet, nicht juristisch.
- **Folge: Abhängigkeit von nachgelagerten Verträgen:** Viele kritische Punkte (z.B. konkreter Einsatz einer OpenAI-Lösung in einem Ministerium) müssten in **separaten Verträgen** oder Ausschreibungen geklärt werden. Das MoU *verdrängt* jedoch möglicherweise reguläre Vergabeprozesse, da die politische Weichenstellung bereits erfolgt ist. So berichtete ein Regierungsinsider zum vergleichbaren Google-

Cloud-Deal, man habe keine Ausschreibung gemacht, da "kein Geld fließt"[29]. Dies schafft einen **Präzedenzfall**, der normale Beschaffungsregeln umgeht, solange Leistungen „kostenlos“ angeboten werden – eine Grauzone ohne parlamentarische Kontrolle.

Bewertung: Die Freiwilligkeit des MoU gibt beiden Seiten Flexibilität, doch sie schafft ein **Governance-Vakuum**. OpenAI erhält politischen Zugang und Einfluss, ohne vertragliche Pflichten; die Regierung kann zwar prinzipiell andere Anbieter prüfen, ist aber de facto moralisch gebunden, OpenAI den Vorzug zu geben (aufgrund der politischen Symbolik der Partnerschaft). Sollte es zu Pannen oder Unstimmigkeiten kommen, droht ein **Schuldvakuum**: Wer trägt Verantwortung, wenn z.B. ein KI-System Fehlentscheidungen trifft? Das MoU trifft dazu **keine Aussage** – die Haftung bliebe vermutlich beim Staat hängen, da OpenAI mangels Vertrag kaum haftbar gemacht werden kann. Dieses Thema der **Haftungsfragen** bei KI-Fehlentscheidungen wird unten (3.3) vertieft.

3.2 Vage Formulierungen und fehlende Spezifika

Das MoU ist in weiten Teilen **absichtlich vage gehalten**. Offizielle Stellen sprechen von einem "Rahmen, um den Dialog zu facilitieren"[35]. Doch diese Vagheit birgt Risiken:

- **Breiter Anwendungsbereich ohne Priorisierung:** Das MoU listet zahlreiche Bereiche auf – von Verwaltung über Justiz bis Verteidigung – in denen KI „Potenzial“ habe[36]. Es fehlen jedoch **präzise Ziele oder Metriken**. Weder sind konkrete Pilotprojekte benannt, noch gibt es Erfolgskriterien zur Messung des Fortschritts (siehe Leitfrage 1 in Kap. 9). Alles ist dem vagen Motto untergeordnet, Möglichkeiten zu „identifizieren“[37]. Regierungsvertreter feiern dies als flexibel, Kritiker bemängeln einen **Mangel an Fokus und Verbindlichkeit**. Selbst Regierungsmitglieder äußerten Unzufriedenheit über die fehlende Spezifik im Abkommen[34].
- **Keine Regeln zu Daten & IP-Rechten:** Das Dokument schweigt zu wesentlichen Governance-Punkten wie **Datenteilung, Datenschutz und geistigem Eigentum**. Beispiel: Wenn britische Behörden OpenAI-Modelle nutzen und dafür eigene Datensätze einspeisen, bleibt unklar, wem daraus entstehende **Modelverbesserungen** gehören. Ohne vertragliche Regelung könnte OpenAI z.B. aus dem UK-Polizeidatensatz gelernte Erkenntnisse in kommerzielle Produkte einfließen lassen, **ohne Entschädigung** oder Mitsprache des UK. Solche Lücken bergen langfristig die Gefahr, dass **öffentliches Wissen privatisiert** wird.

- **Keine Erwähnung von Standards oder Prüfkriterien:** Anders als etwa der EU AI Act definiert das MoU **keine technischen Standards** oder Auditprozesse für KI-Systeme. Etwaige **Bias-Prüfungen, Sicherheits-Checks oder Zertifizierungen** für die in Behörden eingesetzten Modelle werden nicht erwähnt. Es wird nur allgemein darauf verwiesen, man wolle im Einklang mit britischen Sicherheitsstandards handeln[38] – welche das sind, bleibt offen. Ohne klare Vorgaben besteht die Gefahr, dass **proprietäre Prüfkriterien** von OpenAI dominieren und der Staat wenig Einblick erhält.
- **Unbestimmte Versprechen seitens OpenAI:** OpenAI sichert im MoU nichts Konkretes zu – außer dem Willen zur Kooperation. Aussagen wie die mögliche Beteiligung an Rechenzentren oder die Erweiterung des Londoner Büros sind **unverbindlich**[9][39]. Für die Regierung ist es politisch heikel, wenn diese Versprechen ausbleiben. Zum Vergleich: Microsoft und Google haben in ähnlichen Fällen oft zunächst PR-wirksam Investitionen angekündigt, die dann teilweise ausblieben oder viel kleiner ausfielen als propagiert. Hier fehlt ein Mechanismus, um **Versprechen in verbindliche Zusagen** zu überführen.

Governance-Fazit: Die rechtliche Konstruktion des MoU – freiwillig, unverbindlich, breit formuliert – ermöglicht zwar schnelle Kooperation, hebt aber **übliche Kontrollinstanzen** aus. Im Westminster-System werden große IT-Projekte normalerweise vom Parlament oder wenigstens von Ausschüssen begleitet. Hier entstand quasi **am Parlament vorbei** eine weitreichende Public-Private-Partnership. Diese Intransparenz beim Zustandekommen (siehe unten 3.4) und die beabsichtigte Umgehung formaler Vergabeverfahren (Stichwort „kein Geld, kein Tender“) verletzen Grundsätze von **Good Governance**. *Expertinnen fordern daher, künftige Schritte aus dem MoU – z.B. konkrete Pilotprojekte – formalisiert auszuschreiben und parlamentarisch zu überwachen**, um die vagabundierende Struktur etwas zu bändigen[40].

3.3 Haftungsfragen bei KI-Fehlentscheidungen

Ein kritischer, bisher ungelöster Punkt sind **Haftungsfragen**, wenn KI-Systeme im öffentlichen Dienst falsche oder schädliche Entscheidungen treffen. Beispiele könnten sein: Ein KI-Tool zur Haftentlassungsprognose begeht einen schweren Fehler; ein automatisierter Verwaltungsassistent verweigert unrechtmäßig Leistungen an Bürger. Im aktuellen Setup stellen sich folgende Probleme:

- **Unklare Verantwortlichkeit:** Wenn Behörden OpenAI-Modelle einsetzen, liegt die **Entscheidungsverantwortung** formal bei der Behörde. Doch praktisch stützen sich

Beamte auf KI-Ergebnisse. Wer haftet etwa, wenn ein **BIAS** im OpenAI-Modell zu diskriminierenden Entscheidungen führt (z.B. höhere Ablehnungsquote für bestimmte Gruppen)? Der Staat könnte verklagt werden (etwa wegen Ungleichbehandlung), hat aber gegenüber OpenAI mangels Vertrag kaum Regressmöglichkeiten.

- **Fehlende vertragliche Haftungsklauseln:** In klassischen Softwareverträgen gibt es Gewährleistungen oder Haftungsbegrenzungen. Hier fehlt jegliche Regelung. OpenAI bietet seine Dienste meist über API-Nutzungsbedingungen an, die **Haftung stark ausschließen** und Nutzung „as is“ bereitstellen. Sollten Behörden diese AGB akzeptieren, würden sie faktisch anerkennen, dass **OpenAI nicht haftet**, selbst wenn dessen Modell grob fehlerhaft arbeitet. Die öffentliche Hand trägt dann allein das Risiko – und damit letztlich die Steuerzahler oder Geschädigten.
- **Keine Pflicht zu Transparenz/Audits:** Ohne vertragliche Verpflichtung muss OpenAI im Schadensfall **keine Einsicht** in sein Modell gewähren. Weder Behörden noch Gerichte könnten den zugrundeliegenden Code oder Trainingsdaten einsehen, da es sich um Betriebsgeheimnisse handelt. Dies erschwert die **Aufklärung von Vorfällen** immens. Beispiel: Sollte ChatGPT in einem Behörden-Chat falsche amtliche Auskünfte geben, wäre es schwierig nachzuvollziehen, ob ein Modellfehler oder falsche Nutzung vorlag – eine Grauzone, die Verantwortungsdiffusion begünstigt.
- **Behörden als letzte Instanz verantwortlich:** Nach aktuellem Verwaltungsrecht haftet die Behörde für ihre Entscheidungen, egal ob sie Tools nutzte. Das bedeutet, **der Staat trägt das Endrisiko** aller KI-Pannen. Das könnte bei schweren Fehlern (z.B. Justizirrtümer durch algorithmische Empfehlungen) politisch äußerst brisant werden. Ohne klare Haftungsregeln droht im schlimmsten Fall ein **Vertrauensverlust** in öffentliche KI-Systeme, weil unklar ist, ob Betroffene angemessen entschädigt werden und ob solche Fehler systematisch aufgearbeitet werden.

Regulatorische Leerstelle: Es zeigt sich ein generelles Fehlen von **Regeln für KI-Haftung** im öffentlichen Sektor. Weder das MoU noch bestehende britische Gesetze geben hier konkrete Leitlinien. Denkbar wäre, spezielle „**Algorithmic Accountability**“-Gesetze zu erlassen, die vorschreiben, dass Behörden bei KI-Einsatz immer eine „menschliche Letztentscheidung“ wahren und im Fehlerfall regress auf den Anbieter nehmen können. Solange dies fehlt, besteht ein erhebliches Risiko, dass **KI-Fehlentscheidungen in kritischen Bereichen (Justiz, Gesundheit) zu Rechtsstreitigkeiten und Vertrauenskrisen** führen. Das MoU hätte – wenn es verbindlicher wäre – hier ansetzen

können, indem es OpenAI zur Zusammenarbeit bei **Fehleranalyse und -haftung** verpflichtet. Die aktuelle Formulierung lässt diese Fragen offen, was als erhebliches Versäumnis zu werten ist.

3.4 Transparenz des Entscheidungsprozesses und Governance

Bereits kurz nach Ankündigung des MoU wurden **Transparenzdefizite** kritisiert: Wie kam der Deal zustande, welche Stakeholder wurden einbezogen, und welche Zugeständnisse wurden gemacht? Zu beleuchten sind:

- **Nicht-konsultierte Stakeholder:** Weder das Parlament noch unabhängige Gremien (etwa der Chief Scientific Advisor oder Datenschutzbeauftragte) waren in die MoU-Verhandlungen sichtbar involviert. Parlamentarier wie Chi Onwurah bemängelten, dass **keinerlei öffentliche Debatte oder Ausschreibung** stattfand[11][12]. Auch Vertreter der britischen KI-Startup-Szene und Zivilgesellschaft wurden vor vollendete Tatsachen gestellt. Dies nährt den Vorwurf, die Regierung habe **hinter geschlossenen Türen mit Big Tech kungelt**, was im Widerspruch zu Prinzipien der offenen, demokratischen Entscheidungsfindung steht.
- **Interessenkonflikte und persönliche Verbindungen:** Peter Kyle, der federführende Technologieminister, pflegt enge Kontakte zu US-Techfirmen. Presseberichte weisen darauf hin, dass **Absprachen mit OpenAI und Google** teilweise informell erfolgten und Kyle eine sehr „tech-freundliche“ Haltung zeigt[29]. Seine frühere Nähe zu Lobbyisten aus dem Silicon Valley wird kritisch gesehen – der **Anschein von Befangenheit** entsteht, wenn lukrative „Partnerschaften“ ohne Wettbewerb an diese Firmen gehen. Dieser Interessenkonflikt könnte erklären, warum standardmäßige Vergabeverfahren umgangen wurden. Good Governance erfordert hier eigentlich **größere Distanz** oder zumindest einen unabhängigen Review der Abkommen.
- **Intransparenz des Abkommens selbst:** Zwar wurde ein **Pressestatement** veröffentlicht und das MoU-Framework in groben Zügen öffentlich gemacht[41][37], doch Details über operative Implementierung fehlen. Parlamentarier fordern die **vollständige Veröffentlichung** des MoU-Textes und aller Nebenabsprachen[40]. Bis dato ist unklar, ob z.B. **Geheimchutz-Aspekte** berücksichtigt wurden (gerade in Verteidigung/Innere Sicherheit) oder ob es **mündliche Gentlemen’s Agreements** gibt, die nicht verschriftlicht wurden. Diese Unklarheit schürt Misstrauen. Foxglove-Direktorin Martha Dark kommentierte, dies sei wieder ein Beleg für die **"leichtgläubige Annäherung"** der Regierung an die vollmundigen Versprechen von Big Tech[42][34].

- **Fehlende demokratische Kontrolle:** Normalerweise würde ein so weitreichendes Vorhaben – KI in Justiz und Verwaltung – durch Ausschüsse begleitet oder in Pilotprojekten evaluiert, bevor flächendeckende Implementierung erfolgt. Hier hingegen wird vieles ins **Ermessen der Exekutive** gestellt, ohne direkte Rechenschaftspflicht. Zwar betont DSIT, jede konkrete Maßnahme würde noch die "üblichen robusten Prozesse" durchlaufen[43], doch der initiale strategische Pfad wurde ohne diese Prozesse festgelegt. Dies kann als **Umgehung parlamentarischer Mitbestimmung** gewertet werden. In Anbetracht der Tragweite (potenziell veränderter Arbeitsweisen tausender Beamter, neue Risiken für Bürgerrechte) wird die Forderung laut, zumindest im Nachgang **demokratische Safeguards** einzubauen – z.B. regelmäßige **Berichtspflichten** der Regierung ans Parlament über den Fortschritt der KI-Integration, Einrichtung eines **unabhängigen Beirats** für KI im öffentlichen Sektor, etc.

Zusammenfassend zeigt die rechtlich-governance Analyse erhebliche **Schwachstellen:** Ein nicht bindendes MoU ohne Durchsetzungsmöglichkeiten, gepaart mit vagen Zielen, unklarer Haftung und intransparenter Genese, schafft ein fragiles Gerüst. Kurzfristig mag es politische Handlungsfähigkeit demonstrieren, langfristig könnte es zu **Chaos bei der Verantwortlichkeit, Vertrauensverlust** in öffentliche KI-Systeme und **Machtasymmetrien** zugunsten von OpenAI führen. Im schlimmsten Fall droht ein Szenario, in dem die Regierung **Kontrolle abgibt**, ohne vertraglich etwas in der Hand zu haben. Dies untermauert die Notwendigkeit, in den folgenden Kapiteln insbesondere **Daten- und Souveränitätsfragen** sowie **Abhängigkeitsrisiken** genauer zu analysieren – und anschließend mit geeigneten **Gegenmaßnahmen** zu beantworten (siehe Kapitel 10).

4. Der Daten-Souveränitäts-Komplex

Eine zentrale Sorge bei der OpenAI-Partnerschaft ist, ob und wie Großbritannien die **Hoheit über staatliche Daten** wahren kann. Dieser „Daten-Souveränitäts-Komplex“ umfasst mehrere Facetten: den Umfang staatlicher Datenzugänge für OpenAI, Konflikte zwischen britisch/europäischem Datenschutzrecht und dem US-Rechtsrahmen, Urheberrechtsfragen beim KI-Training mit britischen Inhalten sowie die Transparenz und Kontrolle aus Bürgerperspektive.

4.1 Umfang und Kategorien staatlicher Datenzugriffe für OpenAI

Das MoU selbst enthält **keine expliziten Bestimmungen**, welche Daten OpenAI erhalten darf oder wie Datenaustausch geregelt wird. Offiziell betont DSIT, das Abkommen *verleihe OpenAI keinen automatischen Zugang zu Regierungsdaten*[44]. Jeder konkrete

Datentransfer müsse gesondert geprüft und datenschutzkonform genehmigt werden[43]. Dennoch ist bereits jetzt klar, dass für sinnvolle KI-Anwendungen ein gewisser **Datenfluss** von Behörden zu OpenAI nötig sein wird:

- **Behördliche Dokumente und Schriftstücke:** Um Modelle für Verwaltungsaufgaben zu feintunen, könnten Regierungsdokumente (Berichte, Anträge, Formulare) als Trainingsmaterial dienen. Diese könnten **vertrauliche Informationen** enthalten. Unklar ist, ob solche Daten auf OpenAI-Servern verarbeitet würden oder ob OpenAI-Modelle ins Regierungsnetz gebracht werden (letzteres wäre datenschutzfreundlicher, ist aber technisch anspruchsvoll).
- **Justiz- und Polizeidaten:** Der Einsatz in der Justiz (z.B. Analysen von Urteilstexten) oder innere Sicherheit würde hochsensible Daten involvieren (Strafregister, Gerichtsentscheidungen). Ein Transfer an OpenAI würde extreme **Datenschutz- und Sicherheitsfragen** aufwerfen. Das MoU erwähnt zwar diese Bereiche als Kooperationsfelder[36], aber nicht, wie Daten dafür genutzt werden. Hier wären strikte Einschränkungen nötig (z.B. nur anonymisierte, aggregierte Daten).
- **Bürgerdaten in Verwaltungsvorgängen:** KI-Assistenten wie „Humphrey“ interagieren mit **Bürgeranfragen, Formularen und Antworten**. Bereits wird GPT-4 im Tool *Consult* eingesetzt, um öffentliche Konsultationsantworten auszuwerten[6]. Dabei fließen Inhalte von Bürgerinnen (*Meinungen, möglicherweise persönliche Angaben*) durch OpenAI-Systeme. *Es ist essentiell zu klären, ob diese Texte das Land verlassen** oder wie lange sie gespeichert werden.
- **Gesundheits- und Sozialdaten:** Sollte – wie angedeutet – KI bei NHS oder Sozialbehörden helfen („fixing the NHS“ als Ministerziel[19]), stünden **medizinische Daten oder Sozialleistungsdaten** im Raum. Diese unterliegen strengem Schutz (Arztgeheimnis, etc.). Jegliche Verwendung durch OpenAI müsste anonymisiert und zweckgebunden erfolgen. Hier wäre Transparenz gegenüber Patienten/Bürgern unabdingbar, doch bisher fehlt jede Ankündigung in diese Richtung.

Datenkategorisierung & Zugriffsrechte: Es bedarf einer **Klassifizierung**, welche Datenkategorien *potenziell* mit OpenAI geteilt werden dürfen. Denkbar ist folgendes Schema:

- **Öffentlich verfügbare Daten:** z.B. Gesetzestexte, Parlamentsdokumente, Open Government Data. Hier wäre eine Nutzung relativ unkritisch, zumal sie häufig unter Open License stehen. OpenAI könnte solche Daten nutzen, um Modelle an britischen Rechts- oder Verwaltungsstil anzupassen.

- **Verwaltungsinterne Daten (ohne Personenbezug):** z.B. Prozessbeschreibungen, Organigramme, interne Statistiken. Diese könnten unter NDA mit OpenAI geteilt werden, um maßgeschneiderte Lösungen zu entwickeln. Risiko: Potenziell **VS-NfD** (Verschlussache – nur für den Dienstgebrauch) könnte dabei sein, was Klärung erfordert.
- **Personenbezogene Daten (Bürgerdaten):** Hochproblematisch, da hier Datenschutz (UK GDPR) greift. Eine Weitergabe an OpenAI wäre nur zulässig, wenn Rechtsgrundlage, Einwilligung oder strikte Anonymisierung vorliegen. Bisher gibt es **keine Hinweise**, dass breite Bürgerdaten an OpenAI fließen sollen – DSIT dementierte dies vorerst ausdrücklich[43]. Allerdings kann durch indirekte Nutzung (Modelle, die mit Personendaten trainiert wurden) ein **Graubereich** entstehen.

Die Forderung der Opposition lautet, die Regierung solle **klar offenlegen**, welche Daten OpenAI für Trainings- oder Betriebszwecke erhalten könnte[11][12]. Ein Vergleich wurde gezogen: *"die Regierung hat einen Schatz an öffentlichen Daten, der für OpenAI enorm wertvoll wäre"*[45]. Genau dieser Schatz – z.B. Millionen Dokumente, die KI-Modelle verbessern könnten – weckt Begehrlichkeiten. Ohne Regeln könnte OpenAI im Extremfall *de facto* Zugang zu Big Data Pools erhalten, was einem **Ausverkauf staatlicher Daten** gleichkäme.

4.2 UK/EU-Datenschutz vs. US-Rechtslage (CLOUD Act, FISA)

Ein Kernproblem der Zusammenarbeit mit einem US-Unternehmen wie OpenAI ist die **jurisdiktionale Kluft**: Britische (und weitgehend EU-äquivalente) Datenschutzstandards stehen potenziell im Widerspruch zu US-amerikanischen Überwachungsgesetzen. Relevant sind vor allem:

- **US CLOUD Act (2018):** Er ermöglicht US-Behörden Zugriff auf Daten, die von US-Unternehmen **im Ausland** gespeichert werden, per Herausgabeanordnung[46][47]. Das heißt: Selbst wenn OpenAI Daten in einem britischen Rechenzentrum hält, könnte theoretisch ein US-Gericht anordnen, diese herauszugeben – beispielsweise für Ermittlungen. Großbritannien hat zwar ein bilaterales Abkommen (UK-US Data Access Agreement) abgeschlossen, aber grundsätzlich bleibt das Spannungsverhältnis: US-Recht kann hiesigen Datenschutz unterlaufen.
- **FISA §702:** Erlaubt US-Geheimdiensten die **Überwachung von Nicht-US-Bürgern** über US-Unternehmen ohne individuellen Gerichtsbeschluss[46][47]. Wenn OpenAI also Kommunikation oder Daten britischer Nutzer verarbeitet, könnten US-Behörden legal darauf zugreifen, sofern es als außenaufklärerisch relevant gilt. Dies

geschieht im Verborgenen und meist mit Geheimhaltungsverfügungen (Gag Orders), d.h. weder der Betroffene noch das Unternehmen dürfen etwas offenlegen[48].

- **UK/EU Datenschutzregeln:** Im UK gilt weiterhin ein Data Protection Act basierend auf der früheren EU-DSGVO. Dieser verlangt, dass personenbezogene Daten nur bei angemessenem Schutzniveau ins Ausland gehen dürfen. Die USA gelten **nicht als datenschutzadequat** (kein Privacy Shield mehr, und UK hat noch keine separate Angemessenheitsentscheidung für die USA). Zwar könnte man Datenverarbeitung auf Standardvertragsklauseln stützen, aber **Geheimzugriffe durch CLOUD/FISA** wären damit nicht abgedeckt, da sie diesen Klauseln widersprechen (wie EU-Urteile feststellten).

Konfliktszenario: Sollte OpenAI z.B. britische Regierungsdaten oder Bürgerdaten in die Cloud laden, besteht das **Risiko**, dass US-Behörden diese abgreifen. Microsoft räumte ein, dass **kein US-Cloud-Anbieter garantieren kann**, dass ausländische Daten vor US-Zugriff sicher sind[49]. Ein Vertreter von Microsoft Frankreich sagte offen: "*Nein, ich kann nicht garantieren, dass französische Daten nicht von US-Behörden beschlagnahmt werden*"[3]. Für britische Daten gilt nichts anderes.

Implikationen für digitale Souveränität: Das bedeutet, Großbritannien läuft Gefahr, **indirekt Überwachungszugriff** auf sensible Daten zu erlauben, wenn OpenAI integriert wird. Besonders kritisch wäre dies in Bereichen wie Verteidigung (Geheimhaltungsstufe!), Polizei oder Gesundheitswesen. Es entstünde eine **Abhängigkeit vom Wohlwollen** der USA bzw. vom Vertrauen in deren Rechtsstaat. Dies widerspricht dem Konzept der „**digital sovereignty**“, das eigentlich vollständige Kontrolle über kritische Daten fordert.

Mögliche Gegenmaßnahmen: Theoretisch könnte die Regierung verlangen, dass **alle OpenAI-bezogenen Datenverarbeitungen on-premises oder in einer britischen Cloud** erfolgen, die nicht unter US-Kontrolle steht. OpenAI hat aber (noch) keine britische Tochter, die unabhängig genug wäre. Selbst eine UK-Tochterfirma von OpenAI wäre letztlich US-beherrscht (CLOUD Act fähig). Manche EU-Länder verfolgen Ansätze wie **„Schwarzkasten“-Infrastruktur:** US-Software läuft auf rein europäischer Hardware, betrieben von lokaler Hand – aber selbst das schützt nicht vollständig vor den Rechtsansprüchen. Letztlich konstatiert ein Fachartikel treffend: "*Kein Vertrag oder 'EU data region' kann CLOUD Act oder FISA 702 neutralisieren. Ist der Provider amerikanisch, sind die Daten nie völlig außer Reichweite.*"[4].

Für das UK bedeutet das: Möchte man **britische Bürgerdaten definitiv vor US-Zugriff schützen**, müsste man auf US-Anbieter verzichten oder sie rechtlich zwingen, **Daten autonom in UK zu halten**. Bei OpenAI ist letzteres fraglich machbar. Die Partnerschaft

setzt hier implizit voraus, dass man dem US-Partner vertraut oder das Risiko in Kauf nimmt. Politisch ist dies brisant, da die Regierung einerseits von „Souveränität“ spricht[50], andererseits faktisch die **Einfallstore für fremde Rechtsordnungen** öffnet. Dieser Widerspruch wird in der öffentlichen Debatte bereits hervorgehoben[13][51].

4.3 Urheberrechtsproblematik beim Training mit britischen Daten

Ein weiterer Aspekt der Daten-Souveränität betrifft **Inhalte und Urheberrechte**. OpenAI-Modelle werden durch das Training auf riesigen Datenmengen „gefüttert“. Dabei stellt sich die Frage: Was passiert, wenn OpenAI zum Training **britische Daten** nutzt, die urheberrechtlich geschützt sind?

- **Öffentliche Daten vs. urheberrechtlich geschützte Werke:** Einige Daten, die OpenAI eventuell nutzen will (z.B. Gesetzestexte, Regierungsberichte), sind gemeinfrei oder unter offener Lizenz – hier kein Problem. Aber viele potenziell nützliche Daten (z.B. wissenschaftliche Publikationen, Bücher, Nachrichtenartikel) unterliegen dem Copyright. Das UK diskutiert aktuell, KI-Unternehmen das Training auf solchen Inhalten zu erleichtern. Im April 2025 lehnten OpenAI und Google jedoch einen Vorschlag der britischen Regierung ab, der ein **Opt-out-System** für Rechteinhaber vorsah[52][53]. OpenAI argumentierte, man brauche praktisch eine **breite Ausnahme im Urheberrecht**, sonst sei das Training zu aufwendig[54].
- **Position OpenAIs:** OpenAI vertritt – analog zu den USA – die Auffassung, dass das **Training an urheberrechtlich geschützten Werken gesetzlich zulässig** sein sollte, idealerweise als Fair Use-ähnliche Regel[55]. In UK/EU ist diese Frage aber ungeklärt und umstritten. Kreativverbände laufen Sturm gegen eine Blanko-Ausnahme. Für OpenAI bedeutet dies Rechtsunsicherheit: Dürfen sie z.B. britische Zeitungsarchive nutzen, um ihre Modelle zu verbessern? Aktuell eigentlich nur mit Erlaubnis oder wenn anonymisiert.
- **MoU-Perspektive:** Sollte die Regierung in der Partnerschaft OpenAI **Zugang zu staatlichen Archiven** geben (z.B. britisches Nationalarchiv digital), könnte das Material enthalten, das Dritten gehört (z.B. privat verfasste Studien, Vertragsdokumente). Hier drohen **Urheberrechtsverletzungen**, wenn OpenAI es für KI-Training nutzt, ohne Lizenzen einzuholen. Der „fox in the henhouse“-Vergleich von Foxglove zielte auch darauf: OpenAI könnte UK-Daten aufsaugen, die **kommerziell wertvoll** sind[56], und damit seine Modelle füttern – letztlich zum eigenen Vorteil und eventuell zum Nachteil britischer Rechteinhaber (z.B. Verlage).
- **Internationale Auswirkung:** Wenn OpenAI seine globalen Modelle auch mit britischen Daten trainiert, stellt sich Frage, ob diese Daten dann in Produkte

einfließen, die **weltweit** genutzt werden. Das mag dem UK egal sein, solange kein Rechtsbruch vorliegt, aber es bedeutet: **britisches Kulturgut und Wissen** könnten in OpenAI-Modellen stecken, ohne dass UK-Beteiligte dafür Anerkennung oder Kompensation erhalten. Insofern wirft dies Fragen von **digitalem Kolonialismus** auf: Wer schöpft Wert aus Daten und Inhalten?

Beispiel: Angenommen, britische Universitäten oder Behörden stellen OpenAI große Textkorpora zur Verfügung. OpenAI trainiert GPT-5 damit und das Modell verbessert sich signifikant. OpenAI verkauft dann Zugänge dieses Modells global. Der **Mehrwert fließt an OpenAI/Microsoft**, während UK als Datenlieferant wenig davon hat außer der Nutzung der fertigen API (für die es vermutlich auch zahlen muss).

Urheberrechtlich problematische Fälle sind bereits aus der Praxis bekannt: OpenAIs GPT-4 zeigte sich trainiert an urheberrechtlich geschütztem Material (z.B. privaten Büchern)[57]. In den USA laufen Sammelklagen (von Autoren, Programmierern) gegen OpenAI wegen massenhafter Copyright-Verletzung. Falls OpenAI britische Texte nutzt, könnte ähnliches drohen, sofern UK das nicht legal absichert.

Regulatorische Lage UK: Die britische Regierung steht hier vor einem Dilemma: Will sie **OpenAI entgegenkommen**, um die Partnerschaft attraktiv zu machen, müsste sie eventuell Gesetze lockern (z.B. eine generelle Text&Data-Mining Erlaubnis auch für kommerzielle KI unter bestimmten Auflagen). Das stieße aber auf Widerstand der Kreativindustrie und wäre ein Bruch mit europäischen Konventionen. Google und OpenAI warnten, zu strikte Regeln (Transparenzpflichten, Opt-outs) könnten dazu führen, dass sie den britischen Markt „**depriorisieren**“[54][58]. Dies klingt fast wie eine Drohung: Gebt uns freie Hand beim Training, sonst profitiert ihr nicht von unseren Modellen.

Bürgerperspektive: Auch aus Sicht der Bürgerinnen *gibt es ein Urheberrechtsthema: Falls OpenAI Zugriff auf z.B. Social-Media-Archive britischer Nutzer oder andere von Bürgern erstellte Inhalte bekommt (selbst wenn öffentlich), wirft das ethische Fragen** auf. Die Bevölkerung könnte sich ausgenutzt fühlen, wenn ihre Äußerungen ohne Zustimmung KI-Trainingsmaterial werden.

Zusammengefasst ist die **Urheberrechtsproblematik** ein weiteres Feld, in dem das MoU keinerlei Leitplanken bietet. Hier wäre es sinnvoll, wenn UK zumindest **Transparenz** schafft: Welche Datenquellen werden OpenAI bereitgestellt? Gibt es Kompensationen für Rechteinhaber? Werden sensible Inhalte gefiltert? Ohne solche Maßnahmen droht ein **Vertrauensbruch** sowohl mit Teilen der Wirtschaft (Kreativsektor) als auch mit Bürgern, die um die Verwendung ihrer Daten fürchten.

4.4 Transparenz- und Kontrollmechanismen für Bürger

Der letztliche Maßstab für Daten-Souveränität ist, ob **Bürger*innen nachvollziehen und kontrollieren** können, wie ihre Daten in KI-Systemen verwendet werden. Hier sind einige Punkte relevant:

- **Algorithmic Transparency Recording Standard (ATRS):** Die britische Regierung hat bereits einen freiwilligen Standard eingeführt, wonach Behörden öffentlich dokumentieren sollen, welche algorithmischen Tools sie nutzen und welche Daten einfließen[59]. Wenn OpenAI-Modelle in Behörden genutzt werden, müsste demnach offengelegt werden: Was tut das Modell? Welche Datenbasis hat es? Welche Risiken wurden erkannt? Allerdings ist ATRS bislang nicht verbindlich und wird von vielen Behörden noch nicht konsequent umgesetzt[60]. Es bräuchte eine **Pflicht**, dass jede Verwendung von OpenAI in der Verwaltung dem ATRS folgt – inklusive Publikation der Informationen. Nur so könnten unabhängige Stellen überprüfen, was mit Bürgerdaten geschieht.
- **Einwilligung und Widerspruchsrechte:** Idealerweise sollten Bürger die Möglichkeit haben, **der Nutzung ihrer personenbezogenen Daten** in KI-Systemen zu widersprechen (Opt-out). Beispielsweise könnte jemand nicht wollen, dass seine in Vergangenheit an Behörden übermittelten Daten nun plötzlich in einen Chatbot einfließen. Derzeit existieren solche Mechanismen nicht. Es wäre denkbar, z.B. im NHS-Kontext analoge Lösungen wie bei Gesundheitsdaten (National Data Opt-out) einzuführen, die auch KI-Trainingsdaten umfassen.
- **Auskunftsrechte:** Nach Datenschutzrecht könnte jeder Bürger Auskunft verlangen, ob **seine Daten** bei OpenAI gelandet sind. Praktisch ist das schwer durchsetzbar, wenn Daten in riesigen Trainingsmassen stecken. Aber zumindest für strukturiert übermittelte Datensätze (z.B. alle Anträge auf Leistung X in Jahr Y) könnte ein Bürger wissen wollen: Wurden meine Daten an OpenAI gegeben? Hier müsste die Verwaltung proaktiv informieren oder Anlaufstellen schaffen. Ohne dies besteht ein **Transparenzdefizit**, das das Vertrauen untergräbt. In der Guardian-Berichterstattung wurde betont, dass die Öffentlichkeit kaum überzeugt ist, dass Big Tech „auf ihrer Seite“ steht[61]. Genau solche Transparenzmaßnahmen wären nötig, um Vertrauen zu gewinnen.
- **Unabhängige Aufsicht:** Es stellt sich die Frage, wer die Einhaltung von Datenschutz und Datensouveränität überwacht. Der ICO (Information Commissioner's Office) wäre zuständig, hat aber bisher wenig Konkretes zu KI geäußert. Es wäre sinnvoll, wenn der ICO oder ein neuer **KI-Ombudsmann** regelmäßig Audits durchführt:

Werden die Auflagen eingehalten? Fließen Daten nur so wie versprochen? Ohne unabhängige Kontrolle muss man sich auf Regierungs- und OpenAI-Angaben verlassen – was skeptisch gesehen wird, zumal es in der Vergangenheit IT-Skandale gab (z.B. Post Office Horizon), bei denen Behördenversagen zu großem Schaden führte[62].

Bürgerbeteiligung: Ein weiterer Punkt ist, dass **gesellschaftliche Akzeptanz** für KI im Staatswesen nur entsteht, wenn Bürger einbezogen werden. Bisher scheint das MoU eine Top-Down-Initiative zu sein. Um die Daten-Souveränitätsfragen zu adressieren, könnte man **Bürgerforen oder Konsultationen** durchführen, in denen erklärt wird, welche Daten wofür genutzt werden sollen, und Bedenken aufgenommen werden. Das würde nicht nur Transparenz schaffen, sondern der Regierung helfen, blind spots zu erkennen.

Zwischenfazit Daten-Souveränität: Die Partnerschaft hat an dieser Front zwei Gesichter: Einerseits verspricht sie, dass UK durch Zugang zu OpenAI's Technologien modernisiert wird, andererseits droht ein Stück **Datenhoheit abgetreten** zu werden. Das Spannungsfeld UK/EU-Datenschutz vs. US-Cloud-Gesetze macht deutlich, dass technische Lösungen allein nicht reichen – hier braucht es **politische und rechtliche Vereinbarungen**, eventuell bis hin zu völkerrechtlichen Abkommen, um britische Bürgerdaten zu schützen. Solange diese nicht existieren, läuft UK Gefahr, seine Bürger dem Schutz fremder Rechtsordnungen zu unterstellen, was sich schwer mit dem Anspruch digitaler Souveränität vereinbaren lässt[13].

Im nächsten Kapitel werden die **technologischen Abhängigkeiten** beleuchtet, die aus der Daten- und Infrastrukturintegration entstehen – gewissermaßen die Kehrseite der Medaille: Hat UK noch Kontrolle über die eingesetzten Systeme, oder diktiert der Anbieter den Fahrplan?

5. Technologische Abhängigkeitsrisiken

Die Kooperation mit OpenAI birgt erhebliche **technologische Abhängigkeitsrisiken**. Während kurzfristig der Zugang zu fortschrittlicher KI-Technologie ein Vorteil ist, könnte UK mittelfristig in eine strategische **Lock-in-Situation** geraten, in der es von OpenAI (und dessen Partner Microsoft) technologisch abhängig wird. Dieses Kapitel analysiert potenzielle Lock-in-Mechanismen, fehlende Exit-Strategien, Resilienzfragen bei Systemausfällen sowie die Reversibilität der Integration. Zudem geht es um die **Entscheidungshoheit** über Updates und Änderungen der KI-Systeme – liegt diese noch bei der britischen öffentlichen Hand oder faktisch beim Anbieter?

5.1 Vendor Lock-in durch proprietäre Standards

OpenAI's KI-Modelle (GPT-4, GPT-5 etc.) sind **proprietär**: Quellcode und Trainingsdaten sind geschlossen; Dienste werden über proprietäre APIs bereitgestellt. Durch die Partnerschaft droht:

- **Einseitige technische Abhängigkeit:** Wenn zentrale Regierungsanwendungen auf OpenAI-APIs aufsetzen, wird ein Wechsel zu alternativen Anbietern **technisch komplex**. Beispiel: Falls das Humphrey-System konsequent auf GPT-Funktionalitäten optimiert wird, könnte man nicht einfach auf ein anderes LLM (Large Language Model) wechseln, ohne die Integrationen neu zu entwickeln. Proprietäre Schnittstellen, spezialisierte Anpassungen und eventuell von OpenAI gehostete Modelle schaffen **Wechselkosten**, die einem klassischen Vendor Lock-in entsprechen.
- **Fehlen offener Standards:** OpenAI hat bislang keine vollständigen offenen Schnittstellenstandards vorgelegt. Es gibt zwar Bemühungen, interoperable Formate zu schaffen (etwa das OpenAI-Plugin-Ökosystem), aber letztlich diktiert OpenAI Format und Protocol. Wenn UK nicht parallel auf **offene KI-Standards** setzt, läuft es Gefahr, dass interne Datenformate, Modell-Schnittstellen etc. ausschließlich auf OpenAI-Technik zugeschnitten sind. Dies erschwert die Einbindung anderer Lösungen (z.B. Open-Source-Modelle) erheblich.
- **Komplementärinvestitionen:** Für eine effektive Nutzung von OpenAI in Behörden müssen vermutlich **Schulungen, Anpassungen und Zusatztools** entwickelt werden. Jede Investition – seien es angepasste Softwaresysteme oder fortgebildete Mitarbeiter, die speziell GPT nutzen können – macht einen Anbieterwechsel kostspieliger. Organisationen neigen dann dazu, beim einmal eingeschlagenen System zu bleiben, um die Investition zu schützen (**Pfadabhängigkeit**).
- **Ecosystem-Lock-in:** OpenAI ist eng mit Microsoft verbunden (Azure Cloud, Office-Integrationen). UK nutzt ohnehin stark Microsoft (365 in Behörden). Durch OpenAI könnte sich dieses **Big-Tech-Ökosystem** weiter verfestigen – z.B. ChatGPT in Teams, Copilot für Office etc. Das **Gesamtpaket** wird attraktiv, aber es schnürt UK in ein US-dominiertes Tech-Stack ein. Alternative Ökosysteme (wie Open-Source-Stacks oder europäische Cloudlösungen) bleiben dann außen vor, was die **technologische Souveränität** mindert.

Ein Branchenvergleich macht die Gefahr klar: In der Vergangenheit gerieten Behörden in Lock-in bei z.B. **Microsoft Windows/Office** – das UK zahlte jahrzehntelang hohe Lizenzkosten, da ein Wechsel zu Linux/OpenOffice trotz langfristiger Einsparpotenziale als

zu aufwendig galt. Ein ähnliches Muster droht nun mit **KI-Services**: Hat man sich einmal an GPT & Azure gebunden, wird es schwer, auf z.B. Open-Source-Modelle (wie LLaMa 2 von Meta oder zukünftige UK-eigene Modelle) umzusteigen.

5.2 Fehlende Exit-Strategien und Migrationspfade

Im Erfolgsfall nutzt die britische Verwaltung in einigen Jahren OpenAI-Modelle breit. Doch was, wenn UK aus geopolitischen, wirtschaftlichen oder ethischen Gründen die **Partnerschaft beenden** will (oder OpenAI sich zurückzieht)? Aktuell ist kein klarer **Exit-Plan** erkennbar:

- **Keine vertragliche Exit-Klausel:** Da kein bindender Vertrag existiert, gibt es auch keine vereinbarte Übergangsregel, falls eine Seite aussteigt. Das MoU sagt lediglich, es *beeinträchtigt nicht künftige Beschaffungsentscheidungen*[1] – theoretisch könnte UK also jederzeit doch mit einem anderen KI-Anbieter arbeiten. Praktisch aber müsste es dann **bei Null anfangen**, da OpenAI ja bisher exklusiv eingebunden wurde.
- **Know-how-Verlust:** OpenAI-Ingenieure und -Forscher arbeiten eng mit britischen Teams zusammen. Sollte die Kooperation enden, ginge wertvolles Wissen verloren, falls es nicht ausreichend **internisiert** wurde. Eine Exit-Strategie müsste vorsehen, dass **britische Experten ausgebildet** werden, die die Systeme verstehen und ggf. selber weiterentwickeln könnten. Noch ist unbekannt, ob solche Kapazitäten aufgebaut werden oder ob UK sich auf OpenAI-Personal verlässt.
- **Alternative Systeme bereit halten:** Eine grundlegende Exit-Strategie wäre, parallele **Alternativen** aufzubauen (z.B. ein nationales KI-Modell oder Kooperation mit anderen Partnern). Bisher setzt UK stark auf *einen* Partner (Mono-Kultur). Es gibt zwar Abkommen auch mit Anthropic und Google, aber diese decken andere Nischen ab. Für generative KI im öffentlichen Dienst scheint OpenAI primär. Ohne zweites Standbein (etwa Open-Source-Lösungen in Reserve) steht UK im Falle eines Abbruchs mit **leeren Händen** da.
- **Migrationskosten:** Ein spätere Migration von OpenAI weg hätte Kosten: Systeme umrüsten, Daten migrieren, Mitarbeiter umschulen. Ein Exit-Plan müsste diese Kosten antizipieren und **Ressourcen** vorsehen. Davon ist nichts bekannt. Im Gegenteil, die Regierung vermittelt den Eindruck, fest auf OpenAI zu setzen, was impliziert, dass man **keinen Plan B** aktiv verfolgt.

Resilienzüberlegung: Gute Praxis im IT-Management ist *Avoid single points of failure*. Hier droht OpenAI zum single point of failure zu werden. Der Exit-Fall muss nicht durch

politischen Bruch eintreten – es könnte auch ein **Unternehmensproblem** sein (OpenAI geht insolvent, wird aufgekauft, ändert Geschäftsmodell drastisch). Microsofts Einstieg hat gezeigt, dass OpenAI sich auch in der Unternehmensphilosophie ändern kann (stärker kommerziell orientiert). UK hat darauf wenig Einfluss. Ohne definierte Exit-Strategie läuft man Gefahr, im Krisenfall **ad hoc improvisieren** zu müssen – mit entsprechendem Risiko für Ausfälle in öffentlichen Diensten.

5.3 Resilienz bei Systemausfällen oder Strategieänderungen OpenAIs

Betriebliche Resilienz: Wenn kritische Verwaltungsprozesse auf OpenAI-Modellen laufen, stellt sich die Frage der **Ausfallsicherheit**. Derzeit hostet OpenAI seine Modelle hauptsächlich in US-Rechenzentren (Azure). Es ist zwar geplant, KI-Rechenzentren in UK aufzubauen, aber OpenAI erwartet, dass **Regierung mitzahlt**[63]. Bislang hat UK zwar AI Growth Zones ausgeschrieben, aber ob OpenAI dort investiert, ist unsicher. Sollte ein Cloud-Ausfall (z.B. bei Azure) oder ein **Modellausfall** passieren, wären eventuell viele Behörden gleichzeitig betroffen – ein systemisches Risiko. - Ein Beispiel: Wäre GPT-4 in einer Bürger-Service-App offline, könnten Tausende Anfragen hängenbleiben. Resilienz erfordert Redundanzen (Backup-Systeme, offline-Fallbacks). Die Partnerschaftskommunikation schweigt dazu. Ohne aktives Management droht **Downtime** zu Verwaltungszeiten.

Strategische Resilienz: OpenAI könnte seine Prioritäten ändern. Etwa: OpenAI entscheidet sich, künftige Modelle nicht mehr allgemein verfügbar zu machen, sondern nur speziellen Kunden (etwa aus den USA) vorbehalten. Oder es ändert seine Lizenzbedingungen (z.B. plötzlich hohe Kosten, Einschränkungen für Regierungsnutzung). Da UK keine vertragliche Absicherung hat, müsste es solche Änderungen **hinnehmen** oder kurzfristig Alternativen finden. Das ist eine **Position der Schwäche**. - Denkbar ist auch, dass OpenAI sich gezwungen sieht, aufgrund US-Regularien gewisse Nutzungen einzuschränken (z.B. falls Exportkontrollen für KI kommen, die Anwendungen in Verteidigung betreffen). UK könnte also externen Beschränkungen unterliegen, wenn es auf OpenAI baut.

Upgrades und Änderungen: OpenAI's Modelle entwickeln sich schnell. GPT-4 wird GPT-5 etc. Dabei ändern sich oft Verhaltensweisen. Wer entscheidet, ob und wann britische Behörden ein **Upgrade** machen? Wenn OpenAI z.B. GPT-4 einstellt und sagt „nutzt GPT-5 mit neuen APIs“, muss UK folgen, sonst hat es einen veralteten, vielleicht unsicheren Stand. Das heißt, **OpenAI diktiert den Update-Zyklus**, ähnlich wie Softwarehersteller es tun. Dies kann zu unfreiwilligen Anpassungskosten führen, aber auch zu **funktionalen**

Risiken (neue Version hat neue Fehler oder ethische Probleme). Ohne eigene Einflussnahme ist UK hier **passiver Konsument**.

Kontrollverlust vs. Mitgestaltung: Idealerweise würde UK als Partner gewisse **Mitspracherechte** erhalten – etwa Zugang zu Modelleinstellungen, Möglichkeit, eigene Trainingsdaten einzuspielen oder zumindest bestimmte **Feature-Requests** zu stellen, die im öffentlichen Sektor wichtig sind (z.B. erhöhte Transparenzfunktionen). Ob OpenAI dies bietet, ist unklar. Das MoU erwähnt Informationsaustausch, aber nichts zur **Governance der Technologie selbst**[64]. Echte technologische Souveränität würde bedeuten, UK kann im Zweifel einen Fork oder eigenständigen Betrieb machen. Das ist bei closed-source KI aber ausgeschlossen. Somit begibt sich UK in ein **Hochrisiko-Paket**: Es erhält Leistungsfähigkeit, verliert aber **Steuerungsfähigkeit** über die Tools.

5.4 Reversibilität der Integrationen

Dieser Punkt überschneidet mit Exit-Strategie, fokussiert aber auf die **praktische Umkehrbarkeit**: Wie leicht könnte UK die KI-Integrationen wieder entfernen oder durch andere ersetzen?

- **Tiefenintegration in Prozesse:** Wenn KI einmal integraler Bestandteil von Abläufen wird (z.B. automatische Vorprüfung von Anträgen, Chatbot als Erstkontakt in Behörden), dann ändern sich **Prozesse** und **Personalplanung** entsprechend. Eine Reversierung („zurück zum manuellen Prozess“) wäre mit massiven **Reibungsverlusten** verbunden. Mitarbeiter haben sich an KI-Unterstützung gewöhnt; manche Stellen könnten abgebaut worden sein. Das Zurückrollen würde Zeit kosten und temporär Leistungsfähigkeit reduzieren.
- **Abhängigkeitsschleifen:** In komplexen soziotechnischen Systemen können Abhängigkeiten entstehen, an die man nicht sofort denkt. Z.B. KI generiert Berichte, die dann Input für andere Systeme sind. Wird KI entfernt, muss man Ersatz schaffen, sonst bricht eine Kette. Es drohen **Abhängigkeitsschleifen**, die erst in der Umkehr sichtbar werden. Um Reversibilität zu sichern, müsste man früh **mapping** betreiben: Welche Komponenten sind KI-basiert, was wäre deren Fallback? Ohne diese Dokumentation wird ein Rückbau chaotisch.
- **Kosten- und Zeitfaktor:** Jede Integration kostet Aufwand – den Rückbau kostet mindestens ebenso viel, oft mehr (da Systeme dann größer sind). Diese Opportunitätskosten können dazu führen, dass selbst bei Unzufriedenheit mit OpenAI die Verantwortlichen es eher *laufen lassen*, weil die Reversierung als **zu**

teuer/aufwendig gilt. Es entsteht dann ein **Lock-in de facto**, auch ohne vertraglichen Zwang, allein durch die *Kosten des Wechsels*.

- **Psychologische Lock-in-Effekte:** Nicht zu unterschätzen: Wenn Entscheidungsträger ihre Karriere mit dem Erfolg solcher Projekte verknüpfen, sind sie **wenig geneigt, umzusteuern**, da das einem Eingeständnis des Scheiterns gleichkäme. Dieser Aspekt gehört zum Pfadabhängigkeits-Phänomen: Organisationen neigen dazu, einmal getroffene Technologiewahlen zu verteidigen, selbst wenn objektiv ein Wechsel sinnvoll wäre, weil „sunk costs“ mental wirksam werden.

Best Practice vs. Realität: In der IT-Architektur wird oft Interoperabilität und loser Kopplung gepredigt, um Austauschbarkeit zu ermöglichen. Real haben Regierungen aber oft monolithische Systeme. Zumindest sollte UK *jetzt* schon Voraussetzungen schaffen, um Reversibilität zu erhöhen – etwa **Datenportabilität** (d.h. sämtliche Daten, die OpenAI verarbeitet, auch in UK lesbaren Formaten behalten), modulare Integration (KI als Zusatz, Kernprozess bleibt unabhängig) etc. Ob dies bedacht wird, ist fraglich. Nichts im MoU oder den Statements deutet darauf hin, dass die Regierung auf solche technischen **Vorkehrungen** drängt.

5.5 Entscheidungshoheit über Updates und Systemänderungen

Wie schon angedeutet, stellt sich die Frage: Wer bestimmt über **Änderungen** an den KI-Systemen in der öffentlichen Verwaltung?

- **Proprietäre Modelländerungen:** OpenAI könnte Algorithmen-Updates vornehmen, die Verhalten ändern (z.B. neue Moderationsregeln, veränderte Antwortstile). Ein konkretes Beispiel: GPT könnte anfangen, bestimmte Ausgaben einzuschränken (etwa politisch sensible Inhalte anders zu behandeln, da US-Content-Policies dies vorgeben). Hat das UK eine Möglichkeit, dies zu beeinflussen? Eher nicht, außer es gibt Spezialabsprachen für UK-Modelle. Ansonsten **üibernimmt UK automatisch** jede Änderung, die OpenAI global ausrollt – ob gewünscht oder nicht.
- **Feature Roadmap:** Welche neuen Funktionen entwickelt werden, liegt in OpenAIs Ermessen. Das UK kann Wünsche anmelden, aber keine Anforderungen stellen wie bei einer Auftragsentwicklung. Es **verliert also die Hoheit**, strategisch zu planen: "Wir brauchen KI mit Eigenschaft X im Jahr Y". Wenn OpenAI das nicht im Programm hat, gibt es nur abwarten oder teuer selbst implementieren, was gegen den Sinn der Partnerschaft liefe. Somit begibt UK teilweise seine **digitale Gestaltungsmacht** aus der Hand.

- **Sicherheitsupdates und Patches:** Sollte eine Schwachstelle entdeckt werden (z.B. Datenleck, Jailbreak-Möglichkeit in GPT), ist UK auf **OpenAI's Reaktion** angewiesen. Ein souveräner Ansatz wäre, selbst fixen zu können – hier unmöglich. Das Partnerschaftsnarrativ suggeriert zwar, man arbeite gemeinsam an KI-Sicherheit[64], aber in der Praxis bleibt UK Konsument. Das kann zu **Verzögerungen** führen: Bis OpenAI ein Problem behebt, sind britische Systeme potenziell gefährdet.
- **Governance der KI-Ethik:** Ein heikler Punkt ist, wer entscheidet über die **Werte und Biases** des Systems. Wenn KI in der Verwaltung Entscheidungen unterstützt, müssen normative Setzungen getroffen werden (z.B. wie streng, wie konservativ ist ein KI-Risikoalgorithmus). Solche Parameter sollte der demokratische Prozess bestimmen. Bei einem zugekauften Modell hat UK aber wenig Einsicht, welche Vorgaben im Modell stecken. OpenAI als US-Unternehmen hat ggf. andere Prioritäten (z.B. starken Fokus auf amerikanische Debatten, anderes Verständnis von Datenschutz vs. Sicherheitsabwägung). Es besteht das Risiko, dass **algorithmische Entscheidungen** im UK **value-mismatches** aufweisen, weil sie nicht an britischen Normen ausgerichtet wurden – und UK kann es nur begrenzt ändern.

Gesamtbetrachtung Abhängigkeitsrisiken: Die technologischen Abhängigkeiten verfestigen die bereits unter Governance/Daten diskutierten Risiken. UK droht in eine Lage zu geraten, in der es zwar modernste KI nutzt, aber die Kontrolle über diese Werkzeuge weitgehend abgegeben hat – mit allen Folgen: **Lock-in**, erschwerte Ausstiege, Abhängigkeit vom Goodwill eines Monopol-Anbieters, Verlust an strategischer Autonomie. Dies untergräbt letztlich die **digitale Souveränität**, die man offiziell erhalten will[51].

Ein möglicher Ausweg wäre ein **multivendor-Strategie** oder stärker auf **Open-Source/Kollaborative KI** zu setzen – darauf gehen wir in den Szenarien (Kap. 9) ein. Zunächst betrachten wir jedoch in Kap. 6 die **wirtschaftlichen und wettbewerblichen Folgen**, denn technologische Abhängigkeit hat auch Markt- und Kosteneffekte, die für den UK-Innovationsstandort relevant sind.

6. Wirtschaftlich-wettbewerbliche Folgen

Die Partnerschaft mit OpenAI ist nicht nur ein technisches oder administratives Projekt, sondern hat handfeste **ökonomische Implikationen**. Die Regierung erhofft sich erhebliche Wachstumsimpulse und Produktivitätsgewinne[7][8]. Gleichzeitig steht die Frage, wie sich diese Kooperation auf den **heimischen KI-Sektor** auswirkt: Werden britische Startups und Unternehmen gefördert oder an den Rand gedrängt? Außerdem sind die realen

Investitionen und Marktverzerrungen zu beleuchten sowie mögliche Lock-in-Effekte in wirtschaftlicher Hinsicht (z.B. Abhängigkeit von proprietären APIs mit langfristigen Lizenzkosten). Schließlich wird die Auswirkung auf **Arbeitsplätze im öffentlichen Sektor** diskutiert.

6.1 Prognostizierte Vorteile vs. realisierte Investitionen

Regierungsversprechen: Laut DSIT und Schatzkanzler soll KI – angetrieben durch Partnerschaften wie mit OpenAI – die britische Wirtschaft um **£47 Milliarden pro Jahr** bereichern und die Produktivität um 1,5% jährlich steigern[7][8]. Diese Zahl stammt aus dem AI Opportunities Action Plan und wird als Begründung für die aktuellen Initiativen herangezogen. Zudem wird auf **qualitative Vorteile** verwiesen: effizientere Verwaltung (schnellere Verfahren, weniger Bürokratie), neue hochbezahlte Tech-Jobs in UK (OpenAI will London-Büro ausbauen)[65][66], und Großbritannien als attraktiver Standort für KI-Firmen (First-mover-Advantage in Europa). Kurz: Man malt ein Bild, in dem das MoU ein **Turbo-Booster für Wachstum und Innovation** ist.

Realisierungen bisher: Ein Abgleich: - OpenAI hat angekündigt, die **London-Niederlassung zu vergrößern** und mehr Personal einzustellen[67][39]. Das ist positiv für den Arbeitsmarkt, aber bisher noch im Planungsstadium. Bis dato (Sommer 2025) sind die genauen Zahlen offen – „Details über den Sommer“ hieß es[67]. - **Investitionen in Rechenzentren:** Hier liegt noch viel im Ungewissen. Das MoU sagt nur, man „könnte“ investieren[9]. Der UK hat £2 Mrd. in AI Growth Zones eingeplant, aber hofft auf zusätzliche private Milliarden. Ob OpenAI konkret ein Datacenter baut, hängt wohl davon ab, ob die Regierung **mitfinanziert** (OpenAI hat deutlich gemacht, man suche Regierungen, die selbst investieren[63]). Real gab es Stand 2025 noch keine Ankündigung, dass OpenAI z.B. ein großes Data Center in England oder Schottland bauen wird. Somit ist dieses Versprechen noch unbewiesen. - **Pilotprojekte in Behörden:** Hier sieht man einige Ergebnisse: Der KI-Assistent Humphrey mit dem „Consult“-Modul läuft bereits und hat z.B. die Auswertung einer Konsultation signifikant beschleunigt[6]. Das ist ein *Proof of Concept*, dass KI Effizienz bringt. Aber es ist unklar, ob das OpenAI-Partnerschaftsprodukt ist oder unabhängig entwickelt (Humphrey basiert auf GPT-4, aber diese Nutzung hätte auch ohne MoU stattfinden können, da GPT-4 API kommerziell zugänglich ist). - **Konkreter Mehrwert bisher:** Substanziell neue KI-Anwendungen (etwa in Justiz, Bildung) sind im Juli 2025 noch im Planungsstadium. Es gibt also **noch keine empirischen Belege**, dass die groß angekündigten Produktivitätssteigerungen real eintreten. Kritiker warnen davor, dass diese **Prognosen überzogen** sein könnten – Teile der Verwaltung sind komplex und von KI nicht so leicht zu „revolutionieren“ wie erhofft[68][69]. - **Kostenseite:** Die Regierung investiert

selbst £1 Mrd. in Compute-Kapazität[70][71]. Hinzu kommen ~£750 Mio für den Supercomputer in Edinburgh[70]. Das sind erhebliche öffentliche Ausgaben. Es stellt sich die Frage, ob das **Kosten-Nutzen-Verhältnis** gewahrt ist. Wenn OpenAI doch nicht im großen Stil investiert, hätte der Staat viel Geld ausgegeben, damit ein US-Unternehmen von der Infrastruktur profitiert.

In Summe gibt es eine Diskrepanz zwischen **ambitionierten Versprechen** und dem **Stand der Umsetzung**. Das MoU selbst garantiert nichts. Somit ist es kritisch zu beobachten, ob OpenAI tatsächlich in den nächsten Jahren die versprochenen Investitionen und Initiativen liefert – oder ob das UK am Ende hauptsächlich mit eigenem Geld KI-Infrastruktur geschaffen hat, die dann von OpenAI dominiert wird, ohne dass der volkswirtschaftliche Nutzen die erhoffte Höhe erreicht.

6.2 Einfluss auf heimische KI-Startups und Marktverzerrung

Ein oft genanntes Risiko solcher Public-Private-Partnerships mit Big Tech ist die **Verdrängung lokaler Akteure**. Wie wirkt sich das OpenAI-MoU auf britische KI-Startups und den Wettbewerb aus?

- **Bevorzugung eines großen Akteurs:** Indem die Regierung öffentlich eine strategische Partnerschaft mit OpenAI eingeht, sendet sie ein **starkes Signal**: OpenAI ist der bevorzugte Partner für KI-Lösungen im öffentlichen Bereich. Das könnte z.B. bei künftigen Ausschreibungen zu einer **Wettbewerbsverzerrung** führen. Ein kleineres britisches Unternehmen, das vielleicht ein spezialisiertes KI-Tool für Verwaltungen anbietet, steht im Schatten des „Default“-Partners OpenAI. Selbst wenn formal offen ausgeschrieben wird, könnten Behörden geneigt sein, auf den bekannten Partner zurückzugreifen. Dadurch entsteht ein **Ungleichgewicht** zugunsten OpenAIs, was Markteintritt für Wettbewerber erschwert.
- **Startup-Ökosystem:** Großbritannien hat eine wachsende KI-Startup-Szene (DeepMind, Graphcore etc., wobei DeepMind zu Google gehört). Einige setzen auf **Open-Source-Modelle** oder eigene Innovationen. Wenn nun der Staat massiv OpenAI-Technik nutzt, fehlen diesen Firmen **Anwendungschancen** im großen heimischen Markt. Das birgt die Gefahr von **Crowding Out**: Talent könnte abwandern (z.B. zu OpenAI's London-Büro), Investoren setzen eher auf kooperationsnahe Bereiche (z.B. Firmen, die Services rund um OpenAI anbieten, statt Alternative zu OpenAI zu entwickeln). Langfristig droht eine **Konsolidierung zugunsten US-Konzerne**, während UK eigene Champions verpasst.

- **Abhängigkeit der Privatwirtschaft:** Das MoU adressiert nicht nur den öffentlichen Sektor, sondern auch „Unterstützung für kleine Unternehmen beim Einsatz von KI“[72]. Wenn OpenAI hier federführend berät, könnten KMUs ebenfalls primär OpenAI-APIs nutzen. Das stärkt OpenAIs Marktposition und schwächt evtl. Konkurrenzprodukte. Zwar profitieren die Unternehmen kurzzeitig von günstigen KI-Diensten, aber national führt das zu einer **Symbiose mit monopolartigen Strukturen** – wettbewerblich bedenklich, ähnlich wie Cloud-Monopole heute.
- **Rolle der Wettbewerbsbehörde (CMA):** Die CMA hat sich 2023/24 mit Microsoft-OpenAI befasst, aber kein Verfahren eröffnet, da es als Partnerschaft und nicht als Merger galt[73]. Es gibt aber Stimmen, dass Regulierer solche Abhängigkeiten im öffentlichen Bereich im Blick haben sollten. Wenn der Staat quasi **Marktmacht** an einen Anbieter vergibt, ist das auch ein Wettbewerbspolitik-Thema. Bisher scheint CMA & Co. sich zurückzuhalten, was heißt, diese Effekte könnten ungebremst eintreten.

Internationaler Vergleich: Frankreich z.B. versucht, öffentliche KI-Ausschreibungen offen zu halten und fördert Open-Source-Lösungen (etwa mit Bloom/Lemoine Modellen). UK geht hier einen anderen Weg, riskiert aber, **heimische Innovationskapazitäten** unter dem Glanz des Silicon-Valley-Produkts verkümmern zu lassen. Im TechPolicy-Press-Artikel wird betont, dass solche Deals Big Techs **Marktmacht zementieren** und sie teilweise **jeder Regulierung entziehen**, wenn sie in kritische Infrastruktur eingebettet sind[74]. Genau das wäre für den britischen Markt fatal: Weniger Wettbewerb, weniger Diversität, mehr Abhängigkeit.

6.3 Lock-in-Effekte und API-Abhängigkeiten (Kostenfallen)

Wirtschaftlich relevant sind auch die **Kosten- und Lock-in-Effekte** durch Abhängigkeit von proprietären APIs und Diensten:

- **Künftige Preissetzungsmacht:** OpenAI bietet aktuell manchen öffentlichen Partnern (z.B. im MoU-Kontext oder dem Google-Deal) sehr günstige Konditionen – teils kostenloses Pilotieren. Doch sobald Abhängigkeit besteht, könnte OpenAI die **Preise erhöhen** (ähnlich wie Cloud-Anbieter nach Anfangsangeboten die Gebühren steigern). Dann wäre der Staat als Kunde in der Klemme: zahlen oder Dienste verlieren. Diese **Kostenrisiken** sind derzeit unquantifiziert.
- **Folgekosten Integration:** Oft unterschätzt man die **Betriebskosten**. Auch wenn das Modell an sich existiert, braucht es Anpassung, Testing, Compliance-Aufwand – das alles kostet. Wer trägt's? Vermutlich die Behörden. Wenn aber OpenAI bspw. eine

neue API-Version bringt, die Anpassung erfordert, entstehen wieder Kosten. Über Jahre können so erhebliche Summen anfallen, die im TCO (Total Cost of Ownership) anfangs nicht eingerechnet wurden. Lock-in heißt hier: Man zahlt immer weiter, weil Umstieg teurer wäre.

- **Verhandlungsposition UK:** Da OpenAI kein Vertragspartner mit Verpflichtungen ist, hat UK beim Thema Kosten wenig Druckmittel. Wenn OpenAI z.B. beschließt, spezielle Gov-Features nur in einem Premium-Paket anzubieten, müsste UK sich fügen oder viel Geld in Alternativen stecken. Mit jedem Jahr der Abhängigkeit sinkt die Bereitschaft, letzteres zu tun (siehe Pfadabhängigkeit).
- **Ökonomische Souveränität:** Die fortlaufenden Lizenz- und Nutzungskosten fließen ins Ausland ab (OpenAI/Microsoft, USA). Statt eine heimische KI-Industrie zu füttern, unterstützt UK so die **US-Digitalökonomie**. In moderatem Rahmen normal (weil wir auch andere Software importieren), aber im großen Stil ein Problem für die **Daten-Wertschöpfung**: Daten und Nutzer generieren Profit – wenn der fast ausschließlich ins Silicon Valley geht, verliert UK potenzielle Wertschöpfung im Land.
- **Keine Ausschöpfung von Open-Source-Einsparungen:** Open-Source-Modelle haben keine Lizenzgebühren, können auf eigener Hardware laufen (nach Investition). Viele Unternehmen experimentieren damit um sich aus Cloud-Lockins zu lösen. Wenn UK voll auf proprietär setzt, verzichtet es auf die Chance, **Kosten nachhaltig zu senken**, die ein Open-Source-Weg mittelfristig bieten könnte (auch wenn der initial holpriger ist). Man begibt sich in eine Komfortzone mit späteren **Kostenfallen**.

6.4 Auswirkungen auf öffentliche Sektor-Arbeitsplätze

Eine heikle Dimension: **Automatisierung durch KI** könnte langfristig Arbeitsplätze im öffentlichen Dienst reduzieren oder verändern. Die Regierung betont den positiven Spin – KI übernehme Routine, Mitarbeiter könnten sich Wichtigem widmen^{[75][76]}. Dennoch:

- **Stellenabbau vs. Umschulung:** Wenn z.B. 50% der Routineaufgaben mittels KI erledigt werden könnten (eine Schätzung, dass ein Beamter statt 10 Anträgen nun 30-50 pro Tag schaffen kann mit KI-Hilfe^[76]), dann braucht man theoretisch weniger Personal. Ob die Regierung diese Effizienz in Personalabbau ummünzt, ist politisch sensibel. Aber mittelfristig könnten **Stellen eingespart** werden, was Gewerkschaften alarmiert.

- **Neue Qualifikationsanforderungen:** Öffentliche Angestellte müssten vermehrt **digitale Kompetenzen** haben, KI-Systeme verstehen, ihre Ergebnisse prüfen (Human-in-the-loop). Das erfordert Fortbildungen; wer sich nicht anpasst, könnte abgehängt werden. Hier stellt sich die Frage, ob genügend in **Weiterbildung** investiert wird.
- **Veränderung von Rollenbildern:** Manche traditionelle Rollen (z.B. Sachbearbeiter, die Anträge sichten) könnten stark zurückgehen, während neue (KI-Manager, Datenanalysten) entstehen. Der öffentliche Dienst muss intern **Wandel managen**, was oft schwierig ist in behördlichen Strukturen.
- **Akzeptanz und Motivation:** Wenn KI wie Humphrey als „digitaler Kollege“ eingeführt wird, hängt Erfolg auch davon ab, wie Mitarbeiter das annehmen. Fühlen sie sich entwertet oder entlastet? Das MoU und Begleitprogramme müssten die **sozialen Auswirkungen** mitdenken. Bisher kommuniziert die Regierung eher das Heilsversprechen („kein Jammern, keine Müdigkeit wie menschliche Mitarbeiter“ – ein etwas zynischer Ton, der bereits fiel^[77]). Das kann zu **Widerstand** in der Belegschaft führen, wenn nicht sensibel gehandhabt.
- **Regionaler Arbeitsmarkteffekt:** Sollte KI effizienter machen, könnten etwa in manchen Ämtern Standorte zusammengelegt werden oder weniger Neueinstellungen erfolgen. Für strukturschwache Regionen, wo Behörden ein Arbeitgeber sind, kann das negativ sein. Auf der anderen Seite könnten neue Jobs im KI-Bereich entstehen, aber diese sind oft in Metropolen (London, etc.). Somit könnte KI die **Geografie der öffentlichen Beschäftigung** verändern.

Ökonomisch betrachtet muss man die **Transitionskosten** beachten: Kurzfristig kostet die Einführung von KI Geld (Software, Schulung), mittelfristig verspricht sie Einsparungen. Ob diese realisiert werden oder in bessere Dienstleistungen reinvestiert (z.B. kürzere Wartezeiten statt Personalabbau), ist eine politische Entscheidung. Wenn Einsparungen das Ziel sind (Budgetkürzungen), droht eine **soziale Schieflage**, wie jede Automatisierungswelle.

Zusammengefasst: Wirtschaftlich-wettbewerblich bietet die OpenAI-Kooperation Chancen (Innovation, Wachstum, Effizienz), aber auch erhebliche Risiken: Marktverzerrung zugunsten eines US-Monopolisten, Verdrängung heimischer KI-Firmen, potenzielle Kostenfallen durch Lock-in sowie belastende Auswirkungen auf den Arbeitsmarkt im öffentlichen Dienst. Ein **alternativer Ansatz** – die Förderung offener Plattformen oder mehrere Anbieter – könnte gesünder für den Markt sein. Kap. 9 (Szenarien) wird solche Alternativen beleuchten. Zunächst widmet sich Kap. 7 den **demokratisch-**

gesellschaftlichen Aspekten, denn die Einführung von KI in Staatsaufgaben berührt Grundprinzipien der Demokratie und gesellschaftliche Werte.

7. Demokratisch-gesellschaftliche Dimension

Die Implementierung von KI-Systemen – insbesondere von proprietären, schwer durchschaubaren Modellen – im öffentlichen Sektor wirft bedeutende **demokratische und gesellschaftliche Fragen** auf. Diese reichen von der **algorithmischen Entscheidungsfindung** ohne hinreichende demokratische Kontrolle, über Transparenzkonflikte zwischen öffentlichem Interesse und Geschäftsgeheimnissen, bis hin zur öffentlichen Akzeptanz und potenziellem Widerstand. Zudem muss betrachtet werden, welche Stakeholder im Entscheidungsprozess *nicht* konsultiert wurden und welche Folgen dies für die **Legitimität** des KI-Einsatzes hat.

7.1 Algorithmische Entscheidungsfindung ohne demokratische Kontrolle

Wenn KI-Systeme in Bereichen wie Justiz, Verwaltung, Gesundheitswesen Entscheidungen oder Empfehlungen geben, stellt sich die Frage der **demokratischen Legitimation und Kontrolle** dieser Entscheidungen:

- **Fehlende Rechenschaftsmechanismen:** Traditionell können Bürger Entscheidungen eines Amtes anfechten, es gibt verantwortliche Beamte oder Richter. Bei KI ist oft unklar, **wer verantwortlich zeichnet**. Ein Richter könnte sich etwa auf ein Risikobewertungssystem stützen – am Ende entscheidet zwar der Richter, aber praktisch verlässt er sich evtl. stark auf die KI. Wie kann das Parlament oder die Öffentlichkeit kontrollieren, ob diese KI-basierten Entscheidungen fair und korrekt sind? Ohne **Algorithmus-Audits** und Protokollierung droht eine **Entwertung demokratischer Kontrollketten**.
- **„Black Box“-Problematik:** Proprietäre KI-Modelle sind nicht transparent. Weder Parlamentarier noch die Öffentlichkeit können nachvollziehen, *warum* ein System zu einem bestimmten Schluss kam. Das erschwert **Demokratisierung**: Etwa, wenn KI in der Polizeiarbeit eingesetzt wird (Vorhersagen, wen stärker zu überwachen), könnte das zu systematischen Grundrechtseingriffen führen, ohne dass dies öffentlich diskutiert wurde. Solche verdeckten Mechanismen untergraben das Prinzip, dass **Eingriffe vom Gesetzgeber legitimiert und vom Gericht überprüfbar** sein müssen.
- **Keine gesellschaftliche Debatte vor Implementierung:** Im UK wurden algorithmische Tools teils eingeführt, dann erst bei Skandalen rückwirkend

diskutiert (z.B. das A-Levels Algorithmus-Debakel 2020). Bei OpenAI-Kooperation besteht die Gefahr, dass KI in heikle Felder (Strafjustiz, Sozialhilfe-Entscheidungen) kommt, **bevor** eine breite gesellschaftliche Debatte stattgefunden hat, ob man das will und welche Leitplanken nötig sind. Das MoU spricht zwar von „demokratische Werte hochhalten“ [78], bleibt aber unkonkret. Ohne vorherige Debatte kann der Einsatz von KI als **technokratischer Eingriff** wahrgenommen werden, der über die Köpfe der Bürger hinweg geschieht.

- **Verwässerung politischer Verantwortlichkeit:** Ein weiteres Problem: Politiker könnten versuchen, Verantwortung auf „die KI“ zu schieben: „Computer says no“ – man kennt dieses Phänomen aus Verwaltung („der Computer hat das so entschieden“). Das wäre fatal für die Demokratie, da gewählte Vertreter dann **weniger accountable** sind, Entscheidungen als alternativlos darstellen könnten. Um dem entgegenzuwirken, müsste festgeschrieben sein, dass **immer ein Mensch final verantwortlich** zeichnet und KI nur assistiert. Bisher wird das betont (Stichwort human-in-the-loop), aber ob es gelebt wird, ist offen. Die Erfahrung zeigt, dass bei knappen Ressourcen gern auf menschliche Kontrolle verzichtet wird („die Maschine lag bisher immer richtig“).

7.2 Transparenz vs. Geschäftsgeheimnisse (proprietäre Systeme in der Verwaltung)

Transparenzprinzip des Staats vs. Geschäftsgeheimnis des Unternehmens: Hier prallen zwei Welten aufeinander:

- **Informationsfreiheit und Verwaltungsprinzip:** Bürger haben in Demokratien ein Recht zu erfahren, wie Entscheidungen zustande kommen (z.B. durch FOI-Anfragen). Wenn eine Entscheidung durch einen OpenAI-Algorithmus beeinflusst war, wäre eigentlich Transparenz geboten. Jedoch könnten **OpenAI's Schutzrechte** dem entgegenstehen – der genaue Modellinhalt ist geheim. Firmen argumentieren, Offenlegung würde ihr IP gefährden. Das führt zu Konflikten: Ein Bürger, der z.B. abgelehnt wurde für eine Leistung, könnte fragen: Warum? Wenn die Antwort „der Algorithmus hat das so gewichtet“ lautet, müsste der Bürger eigentlich den Algorithmus prüfen können – was OpenAI nie erlauben würde. Hier entsteht ein **Accountability Gap**.
- **Algorithmic Transparency Standard (ATRS) als Kompromiss:** UKs ATRS (vgl. 4.4) versucht zumindest Meta-Infos öffentlich zu machen (Zweck des Algorithmus, Input-Datenkategorien, grundlegende Funktionsweise). Doch ATRS ist freiwillig und bleibt an der Oberfläche; der *Quellcode oder die Modellparameter* werden nicht

offenbart. Gerade bei Big-Tech-KI bleibt vieles Black Box. Transparenzinitiativen fordern daher, dass **Kerne öffentlich verwalteter Algorithmen Open Source** sein sollten. Das wäre mit OpenAI kaum vereinbar, außer man würde auf deren neue Open-Weight-Modelle (wie GPT-OSS) setzen – aber die Partnerschaft zielt eher auf closed model Nutzung.

- **Interessenskonflikt Staat vs. OpenAI:** Der Staat hat eigentlich den Auftrag zur **Neutralität und Fairness**. Wenn er aber ein kommerzielles Tool nutzt, das evtl. bestimmten Bias hat oder kommerzielle Ziele (z.B. Datensammelei) verfolgt, kollidiert das mit dem öffentlichen Interesse. Und weil der Staat das Tool nicht voll durchschaut, könnte er unbemerkt quasi **private Interessen** begünstigen. Z.B.: OpenAI's Modelle könnten bei Themen, die OpenAI's Geschäftsmodell tangieren (Regulierungsdebatten etc.), subtile Einflüsse haben. Das klingt spekulativ, aber es geht um das Prinzip, dass **Intransparenz Türen für Missbrauch** öffnet.
- **Verlust an öffentlichem Vertrauen:** Sobald Bürger den Eindruck haben, Entscheidungen würden von **undurchsichtigen, privat kontrollierten Systemen** getroffen, schwächt das das Vertrauen in Behörden. Insbesondere marginalisierte Gruppen könnten vermuten (oder es kann tatsächlich passieren), dass die KI ihre Anliegen benachteiligt. Aber sie können es kaum beweisen, da der Code geheim ist. Dieses Ungleichgewicht kann zu **Protesten** führen. In ähnlichen Fällen (z.B. Post Office Horizon Skandal, wo eine Software fälschlich Fehlbeträge anzeigte und unschuldige Postmitarbeiter verurteilt wurden) hat man gesehen, welche dramatischen Folgen Black-Box-Systeme ohne unabhängige Prüfung haben[62]. So etwas muss unbedingt vermieden werden.

7.3 Öffentliche Akzeptanz und Widerstand

Die **öffentliche Meinung** zu KI im Regierungsbereich ist geteilt. Manche sehen Chancen (schnellere Services), andere fürchten um Jobs, Datenschutz und Fehlentscheidungen. Was ist in UK diesbezüglich zu erwarten?

- **Bisherige Reaktionen:** Die OpenAI-Ankündigung erntete durchaus **negative Schlagzeilen** und Kritik aus Zivilgesellschaft[34]. Begriffe wie „Fox in the henhouse“ (der Bock als Gärtner) gingen durch die Medien[42]. Das zeigt Skepsis: Man traut Big Tech nicht unbedingt zu, zum Wohle der Bürger zu handeln. Hier hat die Regierung Überzeugungsarbeit zu leisten, wenn sie Akzeptanz will.
- **Wahrnehmung der Bürger:** Vielen ist KI (ChatGPT etc.) bekannt, aber im Kontext Behörden ist es abstrakt. Problematisch wird es, wenn **erste Zwischenfälle** passieren: z.B. ein KI-Fehler führt zu einem Skandal (falscher Bescheid,

Diskriminierungsvorwurf). Dann könnte schnell eine **Ablehnungshaltung** entstehen („wir wollen keine Maschinenjustiz!“).

- **Soziale Gerechtigkeit:** Ein besonderes Augenmerk richten gesellschaftliche Gruppen auf **Bias**: Wenn KI-Entscheidungen systematisch etwa Minderheiten benachteiligen (wie in den USA z.B. COMPAS bei Bewährungsprognosen Schwarze härter einstuft[10]), würde das zu berechtigtem Protest führen. Die Regierung muss hier extreme Vorsicht walten lassen und **Nachweise für Fairness** erbringen, bevor sie KI breit einsetzt.
- **Nicht-konsultierte Stakeholder:** Wie erwähnt, waren etwa **Gewerkschaften, NGOs, Datenschützer** im Entscheidungsprozess zum MoU nicht oder kaum involviert. Das kann sich nun rächen: Diese Stakeholder könnten mobilisieren gegen einen als elitär empfundenen Tech-Deal. Es gibt bereits Organisationen (Foxglove, Big Brother Watch etc.), die wachsam sind und notfalls rechtliche Schritte prüfen. Insbesondere wenn keine Transparenz kommt, wird der **Druck zunehmen**, offen zu legen, was genau gemacht wird.
- **Demokratische Safeguards als Beruhigung:** Um Widerstand zu minimieren, müsste die Regierung **Safeguards** einführen: z.B. gesetzliche Garantien, dass jede KI-Entscheidung anfechtbar bleibt, KI nie allein über Schicksale entscheidet (keine vollautomatisierten Ablehnungen ohne Mensch), und strenge Tests vor Einführung. Solche Versprechen würden die Akzeptanz erhöhen. Bisher sind sie aber nicht klar formuliert.
- **Generationsfrage:** Jüngere Bürger sind eher technikaffin und eventuell offener, solange Service-Qualität stimmt. Ältere oder tech-skeptische Menschen könnten misstrauischer sein. Das kann gesellschaftlich zu **Akzeptanzgefällen** führen. Die Regierung muss also inklusiv kommunizieren: Warum KI, wie gewährleistet man Fairness? Sonst drohen Legitimitätsprobleme.

7.4 Nicht-konsultierte Stakeholder im Entscheidungsprozess

Diese Thematik wurde teils schon in 3.4 und gerade angerissen: Der Umstand, dass wichtige Stakeholder nicht gefragt wurden, hat Konsequenzen:

- **Demokratiedefizit:** Wenn eine so weitreichende Partnerschaft ohne Parlamentsdebatte oder öffentliche Konsultation initiiert wird, fühlen sich viele Akteure **übergangen**. Das schadet der demokratischen Kultur – Transparenz und Beteiligung hätten das Projekt vielleicht besser abgestützt.

- **Potenzial verpasster Expertise:** In UK gibt es renommierte Institute (Ada Lovelace Institute, Turing Institute etc.), die sich mit KI-Ethik beschäftigen. Hätten diese früh einbezogen werden können, wären möglicherweise einige der erwähnten Risiken besser adressiert (z.B. ethische Frameworks). Indem man sie nicht offiziell konsultierte, hat man möglicherweise Know-how verschenkt.
- **Später Protest statt frühzeitiger Konsens:** Stakeholder, die nicht einbezogen wurden, äußern nun öffentlich Kritik (Onwurah, Foxglove etc.). Die Debatte findet also *nach* der Entscheidung statt, was zu konfrontativerem Verlauf führt, als wenn man früh im Dialog Bedenken aufgegriffen hätte. Das MoU steht daher unter **Rechtfertigungsdruck**, anstatt auf breiter Legitimation. Für die Umsetzung könnte das hinderlich sein, wenn z.B. Pilotprojekte auf Widerstand vor Ort stoßen (Beispiel: Einführung eines KI-Systems bei der Polizei könnte von Bürgerrechtsgruppen blockiert werden, falls Vertrauen fehlt).
- **Fehlendes Mandat für radikale Änderungen:** Man kann argumentieren, die Regierung hat zwar generell ein Mandat zu regieren, aber bei solch transformativen Schritten (KI in Kernbereichen) wäre eine **breitere Zustimmung** wünschenswert. In einer Demokratie sollte über die *Weichenstellung, wie viel Algorithmus wir wollen*, eigentlich öffentlich beraten werden. Das bisherige Vorgehen hat da Defizite. Dies ließe sich teilweise korrigieren, indem man z.B. eine **parlamentarische Enquetekommission** einsetzt oder Bürgerdialogformate, um nachträglich das Mandat einzuholen. Bisher gibt es dazu aber nichts Konkretes.

Fazit demokratisch-gesellschaftlich: Die OpenAI-Kooperation bewegt sich auf dünnem Eis, was **demokratische Legitimität** angeht. Wenn nicht nachgebessert wird (durch Transparenz, Debatten, Safeguards), droht ein **Vertrauensverlust** der Bevölkerung in die digitalisierten Behörden. Im Extremfall könnte das zu Ablehnung führen, sodass Projekte gestoppt werden müssen. Um dem vorzubeugen, sind klare **demokratische Leitplanken** nötig: von Rechenschaftspflichten über Bürgerbeteiligung bis zu gesetzlichen Grenzen des KI-Einsatzes. Darauf gehen wir in den Empfehlungen (Kap. 10) ein.

Bevor wir zu den Empfehlungen kommen, widmet sich Kap. 8 noch der **geopolitischen Dimension**, um das internationale Bild abzurunden und historische Parallelen zu ziehen, was technologische Abhängigkeiten betrifft.

8. Geopolitische Positionierung

Die Partnerschaft UK–OpenAI ist auch vor dem Hintergrund geopolitischer Überlegungen zu sehen. Sie berührt das Verhältnis UK–USA (“Special Relationship”), die Position

Großbritanniens gegenüber Europa nach dem Brexit sowie den globalen Wettlauf um KI (USA vs. China vs. EU). Zudem lassen sich historische Parallelen ziehen, wie Staaten in der Vergangenheit mit Abhängigkeiten von ausländischer Schlüsseltechnologie umgingen. Dieser Abschnitt beleuchtet, welche **Außenwirkung und strategische Rolle** die Zusammenarbeit hat und ob Großbritannien damit seine Souveränität stärkt oder eher aufs Spiel setzt.

8.1 UK als OpenAI-Brückenkopf nach Europa (Post-Brexit)

Nach dem Brexit sucht Großbritannien nach neuen Wegen, sich als eigenständiger Tech-Hub zu profilieren. Die OpenAI-Kooperation kann man als bewussten Schritt sehen, UK zum **Einfallstor** für US-KI nach Europa zu machen:

- **Umgehung strengerer EU-Regeln:** Die EU plant mit dem AI Act strikte Auflagen für KI, was US-Firmen Sorgen bereitet. UK hingegen setzt auf einen lockereren, pro-innovations Kurs[16]. Für OpenAI bietet London somit einen **freundlicheren Hafen**, von dem aus man Europa bedienen könnte, ohne direkt EU-Recht zu unterstehen. Quasi ein **Singapur-Effekt:** UK als deregulierte Zone vor den Toren der EU. Sollte das KI-Paket UK erfolgreich sein, könnte OpenAI über UK-Installationen eventuell auch EU-Länder (indirekt) versorgen – zum Unmut Brüssels.
- **Attraktivität für Tech-Investments:** Indem UK signalisiert, Big Tech willkommen zu heißen (siehe Deals auch mit Google, Microsoft, Anthropic[31][13]), will es Kapital und Talente anziehen. Das Land positioniert sich als **Gegenmodell** zu einem protektionistischen oder zersplitterten Europa. OpenAI's Wahl, gerade in UK seine erste Auslandsniederlassung zu eröffnen (bereits 2023 geschehen)[67], untermauert das. Insofern ist UK der **Brückenkopf** für OpenAI nach EMEA – eine Rolle, die UK nach Brexit für sich beanspruchen möchte in verschiedenen Bereichen (auch FinTech etc.).
- **Risiko: EU-UK Spannungen:** Diese Strategie birgt aber das Risiko, die Kluft zur EU zu vergrößern. Wenn EU-Partner das Gefühl haben, UK unterläuft gemeinschaftliche Bemühungen (z.B. einen global verantwortungsvollen KI-Einsatz), könnte das politisch belasten. Ein Beispiel: UK und USA weigerten sich, eine internationale Erklärung zu transparentem KI-Einsatz zu unterschreiben[79]. Das kann in EU-Hauptstädten als unsolidarisch gelten. Als Auswirkung könnten EU-Länder misstrauisch gegenüber UK-basierten KI-Diensten werden (ähnlich wie man es bei Datenflüssen in UK nach Brexit hat – EU prüft Angemessenheitsbeschluss, ist aber skeptisch).

- **UK als KI-Vorreiter oder Versuchslabor?** Manche könnten auch sagen: UK macht sich zum **Testfeld** für US-KI-Exporte. Sollte das Experiment scheitern (z.B. große Probleme auftreten), stünde UK isoliert da. Die EU könnte dann umso mehr argumentieren, dass ihr vorsichtigerer Ansatz richtig war. Gelingt es hingegen, könnte UK einen **Soft-Power-Gewinn** verbuchen, indem es zeigt, wie KI gewinnbringend im Staatswesen nutzbar ist, und andere Länder übernehmen seine Modelle (evtl. sogar kaufen Tools, die UK mit OpenAI entwickelt hat). Das ist eine geopolitische Wette.

8.2 Einfluss auf die UK–US “Special Relationship”

Die enge Partnerschaft mit OpenAI reiht sich ein in die Tradition der “Special Relationship” zwischen UK und USA, diesmal im digitalen Bereich:

- **Vertiefung der transatlantischen Bindung:** Politisch dürfte Washington die UK-OpenAI-Kooperation begrüßen. Es passt zur Strategie, **westliche KI-Allianzen** zu formen, um im Wettstreit mit China vorne zu bleiben. UK positioniert sich hier klar an der Seite der USA (die ja OpenAI im weiteren Sinne fördern, z.B. durch freundliche Regulierung). Das könnte UK in künftigen KI-Initiativen der USA (wie gemeinsamen Forschungsprojekten, Standardsetzung) als **Hauptpartner** etablieren.
- **Abhängigkeit von US-Interessen:** Die Kehrseite: UK bindet sich noch enger an US-Tech-Konzerne. Somit importiert es auch deren Abhängigkeiten – z.B. wenn US-Innenpolitik Big Tech bevorzugt, UK wird schwer gegensteuern (TechPolicy Press betonte, dass UK’s KI-Kurs sich stark an US-Vorstellungen orientiert und Regulierung hinten anstellt[80]). Falls irgendwann US-Regierung und OpenAI auf Kurs gehen, der UK-Interessen schadet (z.B. US verbietet Export bestimmter KI wegen Militär, oder verlangt Datenzugriff), hat UK als Juniorpartner wenig Handhabe. Hier zeigt sich ein **Souveränitätsdilemma**: Man gewinnt Einflussnähe, verliert aber Autonomie.
- **Bündnispolitik:** Sollte die Welt sich in KI-Blöcke aufteilen (USA-led vs China-led vs EU?), positioniert sich UK klar im US-Block. Das kann sicherheitspolitische Vorteile bringen (Tech-Sharing, Bevorzugung bei neuen Innovationen), aber auch **Zwang zur Gefolgschaft**. Z.B. wenn USA KI-Export nach China limitieren, muss UK mitziehen, egal ob es eigenständige Position hätte.
- **Politischer Kontext:** Interessant ist, dass der TechPolicy-Artikel die Zusammenarbeit auch in Hinblick auf eine mögliche Trump-Administration (erwähnt 2025, was andeutet: es könnte wieder ein US-Präsident amtieren, der Druck auf Alliierte ausübt) setzt[81]. UK’s tech-politische Entscheidungen könnten dann in

größeren Verhandlungen als **Pfand** dienen (z.B. USA fordern UK auf, bestimmte KI-Regeln nicht zu machen, sonst... etc.). Das ist spekulativ, aber es zeigt, dass so eine Partnerschaft nicht isoliert existiert, sondern Teil globaler Machtspiele sein kann.

- **UK als “Silicon Valley’s ally”:** International könnte UK’s Vorgehen so wahrgenommen werden, dass es sich auf die Seite der großen US-Konzerne schlägt – im Kontrast zu EU, die eher bändigen will. Das stärkt die US-Position (sie können behaupten: seht, ein großes Land geht unseren Weg), aber ob es UK’s Ansehen als eigenständiger Akteur fördert, ist fraglich. Manche Länder (Frankreich, Deutschland) könnten UK eher kritisch sehen als “verlängerten Arm von US Big Tech”. Hier steht also auch **diplomatisches Kapital** auf dem Spiel.

8.3 Vergleich mit KI-Strategien der EU, China und anderen Partnerschaften

Ein kurzer Vergleich: - **EU (AI Act, souveräne KI-Bestrebungen):** EU verfolgt einen wertebasierten Regulierungsansatz: Risikoklassen, Transparenzpflichten, teils Verbot bestimmter KI-Anwendungen (Social Scoring). Zudem gibt es Initiativen, eigene **europäische Modelle** und Rechenkapazitäten zu fördern (GAIA-X Cloud, öffentlich geförderte LLMs wie LEAM). UK geht statt Regulierung den Weg Partnerschaft mit führendem privatem Akteur und weitgehend Selbstregulierung. Vorteil: schneller Fortschritt, Nachteil: potenzielle Abhängigkeit und weniger Schutz. In 10 Jahren wird man sehen, welche Strategie besser fruchtet. - **China:** China hat massiv in eigene KI-Firmen investiert (Baidu, Tencent etc.), die teilweise vergleichbare Modelle wie GPT haben (z.B. Ernie Bot). China koppelt sich weitgehend ab von westlicher KI (kein OpenAI in China offiziell). Sie regulieren KI streng nach polit. Kriterien (Zensur etc.). UK stellt sich dem diametral entgegen: Öffnung zu westlichem Marktführer, kaum inländische Autarkie. Historisch erinnert das an verschiedene Entwicklungsmodelle: eigenständige Entwicklung vs. Technologieimport. UK war traditionell stark durch eigene Forschung (einst Turing, heute DeepMind), aber nun setzt man eher auf Import. Sollte es geopolitisch zu Konflikten kommen, hätte UK allein kaum KI-Souveränität, während China autark wäre. Ein Balanceakt: man gewinnt Top-Technik schnell, aber riskiert strategische Verwundbarkeit. - **andere Partnerschaften:** Interessant sind auch Cases wie **Anthropic und Google Cloud mit UK** – hier gab es ebenfalls MoUs[31]. Die OpenAI-Kooperation ist aber breiter angelegt, beinahe allumfassend. Man könnte es vergleichen mit, sagen wir, **Palantir im NHS** – dort hat UK viel Kritik geerntet für die Idee, einen US-Datenkonzern in Gesundheitsdaten zu lassen. OpenAI im öffentl. Sektor ist ähnlich sensibel. Andere Länder haben teils Partnerschaften: z.B. **Frankreich mit Microsoft/OpenAI** (z.B. was Orange tut[82]), oder

kleinere Staaten mit IBM etc., aber UK's Deal ist in seinem Umfang (landesweiter Ansatz) relativ beispiellos in westlichen Demokratien. Das macht UK zum **Testfall**.

8.4 Historische Parallelen technologischer Abhängigkeiten

Ein Blick in die Geschichte: - **Telekommunikation/5G:** UK's Debatte um Huawei: zunächst war man offen, dann unter US-Druck doch ausgeschlossen. Das zeigt: Abhängigkeit von fremder Tech (China Huawei) wurde als Sicherheitsrisiko gewertet und man kehrte um, obwohl es Kosten verursachte (alte 5G-Ausrüstung rausreißen). Parallele: Jetzt schafft man Abhängigkeit von US-KI – zwar Verbündeter, aber das Beispiel zeigt, wie schwer Loslösen später ist. - **Nukleartechnologie:** Nach WWII war UK anfangs auf US-Know-how angewiesen, baute aber dann eigenes Kernwaffenprogramm aus Sorge, völlig abhängig zu sein. Heute in KI macht UK (noch) nicht das Äquivalent (eigenes „KI-Atomprojekt“), sondern setzt auf US-Kooperation. Könnte es ähnlich wie beim Nuklearprogramm doch irgendwann beschließen, eigene KI-Rüstung zu forcieren? Möglich, wenn die Abhängigkeit als zu kritisch erkannt wird. - **IT/Cloud-Abhängigkeit:** Seit den 2000ern dominieren US-Firmen (Microsoft, Google, Amazon) die IT-Landschaft in Behörden. EU und UK haben in Ansätzen versucht, Alternativen zu fördern, mit begrenztem Erfolg. Die Cloud-Thematik (siehe Cloud Act) zeigt: Europa ist verwundbar, weil keine eigene Hyperscaler. KI könnte ein **Déjà-vu** werden: Statt eigenem GPT setzt man auf US, und später merkt man, man hat den Anschluss beim Aufbau eigener Kompetenzen verpasst. Historisch war Europa bei Internet und sozialen Medien auch Konsument, nicht Produzent. UK setzt diesen Pfad fort, statt zu brechen. - **Luft- und Raumfahrt:** UK war einst führend (z.B. Jet Engine, Concorde mit FR), dann starker Partner der USA in vielen Projekten. Es hat Innovation in einigen Feldern aufgegeben und kauft lieber US-Technik (z.B. Kampffjets F-35 statt eigenständig neu zu entwickeln). KI könnte analog sein: eigene Entwicklung teuer, man schließt sich lieber dem US-Ökosystem an (OpenAI = Lockheed Martin der KI?). Die Lektion: So verliert man aber auch industrielle Fähigkeiten und ist auf Gedeih und Verderb Kunde.

Schlussfolgerung geopolitisch: Die UK–OpenAI-Partnerschaft stärkt zwar kurzfristig UK's Position als *Ort, an dem KI passiert*, aber strategisch verlagert sie **Macht und Wertschöpfung** in die USA. Trotz aller Rhetorik von „Sovereign AI“^[50] tauscht UK ein Stück seiner digitalen Unabhängigkeit gegen einen fragilen Vorteil im KI-Rennen ein^{[13][51]}. Historische Parallelen mahnen, dass Abhängigkeiten selten ohne Folgen bleiben – sei es politischer Druck oder wirtschaftliche Nachteile.

Damit haben wir die sechs geforderten Dimensionen analysiert. Im nächsten Kapitel (9) werden wir basierend auf all diesen Erkenntnissen **Szenarien für die Jahre 2025–2035**

entwerfen, um mögliche Entwicklungspfade aufzuzeigen: von einer OpenAI-dominierten Zukunft bis hin zur Abkehr und Eigenständigkeit. Diese Szenarien helfen, Risiken und Chancen greifbarer zu machen und fließen anschließend in die Formulierung der Empfehlungen ein.

9. Szenario-Entwicklung 2025–2035

Um die möglichen langfristigen Konsequenzen der UK–OpenAI-Partnerschaft abzubilden, werden in diesem Kapitel drei Hauptszenarien entwickelt. Jedem Szenario wird eine **Eintrittswahrscheinlichkeit** (qualitativ: hoch/mittel/niedrig) zugeordnet, basierend auf aktuellen Trends und Annahmen. Zudem werden ein Best-Case und Worst-Case skizziert, die extreme Ausprägungen darstellen. Abschließend erfolgt eine **Risikomatrix**, die die in den Szenarien identifizierten Risiken nach Eintrittswahrscheinlichkeit und Schweregrad einschätzt.

9.1 Szenario "OpenAI-Hegemonie" – totale Abhängigkeit, Kontrollverlust

Beschreibung: In diesem Szenario, das einem Worst-Case nahekammt, entwickelt sich Großbritannien bis 2030 in eine nahezu vollständige **technologische Abhängigkeit von OpenAI**. OpenAI's Systeme sind tief in alle kritischen öffentlichen Dienstleistungen integriert (Verwaltung, Justiz, Gesundheit, Bildung, Sicherheit). Britische Institutionen haben keine ernstzunehmenden Alternativen etabliert.

- **Verlauf:** Die frühen Pilotprojekte sind erfolgreich und man rollt KI-Lösungen flächendeckend aus (Chatbots bearbeiten Großteil der Bürgeranfragen, KI entscheidet mit bei Gerichtsurteilen, etc.). Aufgrund der Effizienz werden Budgets für menschliches Personal gekürzt. OpenAI eröffnet zwar Rechenzentren in UK, aber behält *volle Kontrolle* über die Technologie. Im Jahr 2028 kündigt OpenAI an, GPT-7 nur noch über exklusive Verträge bereitzustellen – UK unterschreibt hohe Lizenzverträge, da ein Ausstieg undenkbar ist.
- **Merkmale: Vendor Lock-in ist maximal:** Migration weg von OpenAI wäre so teuer und disruptiv, dass es keine Option mehr ist. **Datenhoheit** ist praktisch verloren: Große Teile staatlicher Daten liegen in OpenAI-Systemen, teils auch Nutzerdaten, die evtl. für Trainingsupdates verwertet wurden. Durch CLOUD Act & Co. gab es einige Vorfälle, wo Daten an US-Behörden flossen – UK toleriert es zähneknirschend, um die Partnerschaft nicht zu gefährden.
- **Governance & Politik: Politischer Kontrollverlust** zeigt sich, als OpenAI aus Sorge vor Reputationsschäden 2031 einseitig beschließt, bestimmte heikle Anwendungen

(z.B. predictive policing) abzuschalten. Die britische Regierung hat das hinzunehmen, Gesetze können sie kaum erlassen, ohne die Funktionalität zu verlieren, da es keine Ersatzsysteme gibt. UK's Regulierung bleibt lax, faktisch lässt man OpenAI die Spielregeln diktieren (z.B. in KI-Sicherheitsfragen folgt man OpenAI's Empfehlungen blind).

- **Wirtschaft & Gesellschaft: Britische KI-Unternehmen sind weitgehend verdrängt** oder wurden von US-Firmen aufgekauft. Das Versprechen von £47 Mrd. Zusatz-BIP erweist sich als überhöht; zwar steigen Produktivitätskennzahlen etwas, aber der Großteil der Wertschöpfung fließt als Lizenzgebühren ins Ausland. Es kommt zu öffentlichen Protesten, als ein KI-System im Jahr 2032 einen massiven Bias-Skandal auslöst (z.B. Diskriminierungsskandal in der Strafverfolgung) – die Bevölkerung fordert Abkehr, doch die Regierung ist so abhängig, dass sie nur kosmetische Änderungen machen kann.

Wahrscheinlichkeit: *Mittel* (dieses Worst-Case-ähnliche Szenario ist nicht völlig ausgeschlossen, aber die öffentliche und politische Gegenwehr könnte vorher eingreifen).

Folgen: Digitaler **Kontrollverlust** der Demokratie, Souveränitätsverlagerung zu einem Privatkonzern, enormes Risiko für Missbrauch. In der **Risikomatrix** unten erscheinen in diesem Szenario viele Risiken als **hoch** (Datenabfluss, Lock-in, gesellschaftliche Unruhe).

9.2 Szenario "Multilaterale Balance" – diversifizierte KI-Partnerschaften

Beschreibung: In diesem optimistischen Szenario schafft es Großbritannien, die OpenAI-Partnerschaft erfolgreich zu gestalten, ohne einseitig abhängig zu werden. Man etabliert bis 2030 eine **ausgewogene KI-Landschaft**: OpenAI ist ein wichtiger Partner, aber nicht der alleinige.

- **Verlauf:** Nach dem Start mit OpenAI öffnet die Regierung ab 2026 gezielt weitere Partnerschaften – z.B. mit europäischen Open-Source-Konsortien oder anderen US-Anbietern (Anthropic, Google) – für unterschiedliche Anwendungsfälle. Zudem investiert sie in **eigene KI-Kapazitäten**: Ein britisches KI-Forschungszentrum entwickelt ein mittelgroßes Sprachmodell, das in einigen Behörden als Open-Source-Alternative läuft. Die Zusammenarbeit mit OpenAI bleibt bestehen, aber wird formeller: 2027 schließt man einen MoU 2.0 als verbindlichen Vertrag, der Daten, Haftung, etc. regelt und OpenAI verpflichtet, Rechenzentren in UK unter britischem Recht zu betreiben.
- **Merkmale: Diversifikation:** Kein Bereich hängt ausschließlich an OpenAI. Z.B. im Justizbereich nutzt man ein EU-Modell aus Sicherheitsgründen, im Bildungsbereich

OpenAI, in der Verwaltung teils Open-Source. So entsteht eine **Multi-Cloud/Multi-AI-Strategie**. **Datenhoheit** wird verbessert: Durch rechtliche Klarstellungen bleiben sensible Daten in UK-Rechenzentren; der UK-ICO und ein KI-Governance-Board überwachen die Nutzung.

- **Governance & Politik: Demokratische Kontrolle** wird ausgebaut: Bis 2028 verabschiedet das Parlament ein **AI Accountability Act**, der Algorithmen in der Verwaltung Audits und Transparenzanforderungen unterwirft. OpenAI kooperiert, indem es z.B. Schnittstellen für Audit-Institutionen öffnet. Entscheidungen bleiben menschlich verantwortet; es gibt Gremien, in denen Zivilgesellschaft mitredet. So bleibt die **Legitimität** gewahrt, und größere Skandale bleiben aus.
- **Wirtschaft & Gesellschaft: UK-Startups** finden Nischen im OpenAI-Ökosystem oder als Zulieferer für die alternativen Modelle. Das Wachstum im KI-Sektor ist robust, einige britische Firmen exportieren sogar GovTech-Lösungen. Der Prophezeite Produktivitätsschub realisiert sich teilweise (vielleicht £30 Mrd statt 47, aber spürbar). Gleichzeitig gelingen Umschulungen: Der öffentliche Dienst reduziert zwar manche Stellen, schafft aber neue KI-spezifische Jobs (ethics officers, etc.), sodass es **sozial abgefedert** ist. Die Bevölkerung sieht Verbesserungen (schnellere Verwaltung) und durch die Transparenzmaßnahmen bleibt **Vertrauen** bestehen.
- **Geopolitik:** UK wird ein **Vermittler** zwischen USA und EU: Es zeigt, dass man KI nutzen kann und trotzdem Regulierung haben kann. UK beteiligt sich aktiv an globalen KI-Gremien und treibt Standards voran. OpenAI's Präsenz in UK bleibt stark, aber UK behält **Souveränität**, indem es Alternativen in der Hinterhand hat.

Wahrscheinlichkeit: *Niedrig bis mittel* (dies erfordert proaktive politische Steuerung und auch Kooperationswillen, was ambitioniert ist, aber nicht unmöglich).

Folgen: UK nutzt Innovation **ohne Souveränitätsverlust**, kann als Modell fungieren. Risiken wie Lock-in oder Datenschutzverletzungen werden **auf mittel bis niedrig** reduziert, da Gegenmaßnahmen greifen.

9.3 Szenario "Technologische Fragmentierung" – Rückzug und Eigenentwicklung

Beschreibung: In diesem Szenario kommt es zu einer Fragmentierung: Die Partnerschaft mit OpenAI scheitert oder wird stark zurückgefahren bis 2030. Großbritannien orientiert sich um und setzt verstärkt auf **eigene oder alternative KI-Wege**.

- **Verlauf:** Ab 2026/27 häufen sich Probleme und politische Widerstände. Ein Datenskandal (z.B. doch öffentliche Daten in den USA gelandet) führt 2027 zu einem Parlamentsbeschluss, die Zusammenarbeit mit OpenAI **einzufrieren**. UK investiert panikartig in ein „**Sovereign AI**“-Programm, ähnlich wie damals das UK selbst eine Atombombe baute, versucht man nun ein nationales LLM zu entwickeln – teuer und zunächst rückständig. Zwischenzeitlich wird auf Open-Source-Modelle aus EU und Eigenentwicklungen umgestellt, was aber Reibungen mit sich bringt (Systeme laufen schlechter, Übergangschao in Behörden).
- **Merkmale: Fragmentiertes System:** Manche Behörden nutzen noch alte OpenAI-Lösungen, andere sind auf rudimentäre Alternativen gewechselt. Es gibt kein einheitliches KI-Framework mehr; Interoperabilität leidet. **Effizienzverluste** treten auf, da einige Projekte auf Eis liegen.
- **Governance & Politik:** Politisch wurde die Notbremse gezogen aus Souveränitätsgründen. Es gibt nun starke **Regulierung** (vielleicht verabschiedet UK 2028 einen strengen AI-Sovereignty Act), aber das bremst auch Innovation. UK versucht Allianzen mit EU (vielleicht tritt man einem EU-Cloud-Projekt bei) und präsentiert das als *Wiederherstellung der Kontrolle*. Die Regierung zahlt Schadensersatz/Migrationskosten für den Exit aus dem OpenAI-Deal; möglicherweise kommt es zu **Streit mit den USA**, die enttäuscht sind vom Rückzug.
- **Wirtschaft & Gesellschaft:** Kurzfristig negativ: Der KI-Boom flaut ab, manche OpenAI-nahe Startup schließen. Dafür entstehen staatlich geförderte KI-Forschungsprojekte. Möglicherweise fließt viel Steuergeld in das Nachholen dessen, was man nicht selbst entwickelt hatte – **ineffizient, aber souveränitätspolitisch motiviert**. Die Gesellschaft ist gespalten: Einige sagen „gut so, wir wollen keine Black-Box-KI“, andere kritisieren den Verlust an Fortschritt. Die öffentlichen Dienste fallen teils zurück auf manuelle Verfahren oder weniger leistungsfähige KI. Die Bürger spüren das (wieder längere Wartezeiten etc.), aber man verkauft es als Preis für **Datenschutz und Unabhängigkeit**.
- **Geopolitik:** UK nähert sich ggf. der EU-Linie wieder an, rückt von den USA etwas ab. Global wird UK nicht mehr als KI-Vorreiter wahrgenommen, eher als jemand, der zurückruderte. Das kann aber auch Respekt verschaffen bei jenen Ländern, die big tech kritisch sehen (z.B. einige im globalen Süden, die Datenschutz hochhalten).

Wahrscheinlichkeit: *Niedrig* (dies würde einen drastischen Bruch voraussetzen; eher denkbar falls große Skandale oder Regierungswechsel mit radikal anderer Tech-Politik).

Folgen: UK behält formale Souveränität, verliert aber **Innovationsschub** und hat wirtschaftlich Nachteile. Viele Risiken aus der Partnerschaft (Datenabfluss, Bias) sind dann entschärft, aber neue Risiken tauchen auf (z.B. **technologischer Rückstand**, hohe Kosten, isolierte Insellösungen).

9.4 Best-Case und Worst-Case Szenarien mit Risikomatrix

Best-Case (Optimum): Das Best-Case deckt sich im Wesentlichen mit **Szenario 9.2 (Multilaterale Balance)**. Hier nutzt UK KI-Technologie **profitabel und verantwortungsvoll**, wahrt zugleich seine Werte und Souveränität. OpenAI liefert seine Versprechen: investiert in UK, kooperiert konstruktiv an Sicherheitsstandards; es gibt keine größeren Ethik-Skandale. Britische Bürger profitieren durch bessere Services, behalten aber Vertrauen, da Transparenz und Kontrolle gegeben sind. UK's Wirtschaft wächst durch KI-Innovationen, und man bleibt international konkurrenzfähig. Die Partnerschaft wandelt sich in eine für beide Seiten **faire Kooperation** (OpenAI erhält Marktzugang und Unterstützung, UK bekommt Technologie und Investments, ohne untergebuttert zu werden).

In diesem Best-Case sind die **Risiken niedrig**: Daten werden nicht missbraucht, Abhängigkeiten bleiben beherrschbar (weil Alternativen vorhanden sind), gesellschaftliche Akzeptanz ist hoch, und die Demokratie wurde nicht ausgehöhlt.

Worst-Case (Pessimum): Der Worst-Case entspricht dem extremsten Punkt von **Szenario 9.1 (OpenAI-Hegemonie)**, vielleicht noch zugespitzt: Stellen Sie sich vor, es käme zusätzlich zu politischer Einflussnahme (OpenAI könnte – wild spekuliert – mal drohen, Dienste abzuschalten, falls UK gewisse Regulierungen erlässt, was den Charakter einer Erpressung hätte). Oder im schlimmsten Fall würde UK's digitaler Staatsapparat zum **Spielball** in einem USA-China-Konflikt: Sollte es zu Sanktionen kommen, könnte UK den Zugang zu „seiner“ KI verlieren (ähnlich wie gewissen Ländern Softwarelizenzen entzogen werden bei Sanktionen). Dann stünde UK komplett blank da. Das Worst-Case-Szenario wäre also totale Abhängigkeit plus eventuell **Verlust jeglicher Kontrolle**, was praktisch ein Souveränitäts-GAU wäre.

Im Worst-Case sind **fast alle identifizierten Risiken hoch** und realisiert: - Datenabfluss passiert (CLOUD Act-Zugriffe, evtl. Leaks), - Bias und Fehlentscheidungen häufen sich, beeinträchtigen Bürgerrechte, - Lock-in ist unumkehrbar, OpenAI diktiert Preise und Bedingungen, - britische KI-Branche ist kaputt, nur ausländische Konzerne dominieren, - demokratische Kontrolle existiert kaum, evtl. nutzen Autoritarismus-Tendenzen die KI (z.B. Massenüberwachung mit OpenAI-Tools), - im Extrem: Sogar Sicherheit könnte leiden, wenn

z.B. Verteidigungssysteme auf fremder KI basieren (Stichwort Autonomie in Waffensystemen).

Risikomatrix: Basierend auf den obigen Szenarien und Analysen lässt sich eine qualitative Risikobewertung tabellarisch darstellen:

Risiko	Wahrscheinlichkeit	Schadensausmaß (Impact)	Gesamtbewertung
Daten-Souveränitätsverlust (staatliche und Bürgerdaten unter US-Zugriff)	Mittel bis hoch – im Basisszenario wahrscheinlich teils gegeben, außer Gegenmaßnahmen greifen	Hoch – Verletzung von Bürgerrechten, potenziell nationaler Sicherheitsaspekt	Hoch (dringend zu adressieren)[47][83]
Vendor Lock-in / Tech-Abhängigkeit	Hoch – wenn kein Multi-Vendor-Plan, ist Lock-in fast sicher in wenigen Jahren	Hoch – führt zu Kontrollverlust, hohe langfristige Kosten	Hoch (im Worst-Case voll realisiert)[74]
Fehlende Haftung & KI-Fehlentscheidungen	Mittel – Fehler werden passieren; ob Haftungsfall draus wird, hängt von Mechanismen ab	Mittel bis hoch – kann individuelle Schicksale hart treffen, Vertrauensverlust in Institutionen	Mittel-Hoch (muss vorbereitet werden)
Marktverdrängung heimischer KI-Firmen	Mittel – Tendenz erkennbar, aber nicht unausweichlich (abhängig von Polit-Maßnahmen/Förderungen)	Mittel – Verlust von Innovationspotential, aber ggf. Kompensation durch ausländische Investition	Mittel (im Balance-Szenario gering, im Hegemonie-Szenario hoch)
Kostenexplosion durch Abhängigkeit (Lizenz, API-Kosten)	Mittel – OpenAI könnte Preisanhebungen vornehmen in Zukunft	Mittel – belastet Staatsfinanzen, aber finanzierbar, sofern Wirtschaft entsprechend wächst	Mittel

Risiko	Wahrscheinlichkeit	Schadensausmaß (Impact)	Gesamtbewertung
Gesellschaftliche Ablehnung/Widerstand (wegen Intransparenz, Bias)	Mittel – hängt von konkreten Vorfällen ab; initial Skepsis vorhanden[84]	Hoch – kann Projekte stoppen, erfordert Kurskorrekturen, politischer Schaden für Regierende	Mittel (steuerbar durch gute Governance, aber nicht zu ignorieren)
Demokratie-Defizit (schleichende Erosion von Kontrolle, Black-Box-Entscheidungen)	Hoch – wenn keine Gegenmaßnahmen, kommt es schleichend (ist schwer messbar, daher Gefahr wird oft unterschätzt)	Hoch – Fundament der demokratischen Legitimität betroffen	Hoch (eine der kritischsten langfristigen Folgen)
Geopolitische Verwundbarkeit (UK als Spielball US-Techpolitik)	Mittel – derzeit enger Schulterschluss mit USA, kann zum Nachteil werden falls Interessen divergenzieren	Mittel – je nach globaler Lage (Konflikte), könnte UK gezwungen werden, unsouveräne Entscheidungen zu treffen	Mittel (in Balance-Szenario gering, in Hegemonie-Szenario hoch)
Technologischer Rückstand bei Bruch (Falls Wechsel zu Open-Source nötig)	Niedrig – tritt nur im Fragmentierungs-Szenario ein	Mittel – würde einige Jahre dauern aufzuholen, aber temporär	Niedrig (vermeidbar durch kluge Strategie)

(Legende: "Wahrscheinlichkeit" und "Impact" qualitativ eingeschätzt für den Zeithorizont bis 2035. "Gesamtbewertung" als Priorität, Handlungsbedarf.)

Diese Matrix zeigt: Besonders dringlich sind Risiken um **Souveränität, Lock-in und Demokratie** („hoch“ bewertet). Viele andere liegen im mittleren Bereich und lassen sich durch proaktive Politik mildern.

Im nächsten abschließenden Kapitel werden auf Basis dieser Erkenntnisse **Handlungsempfehlungen** ausgesprochen, wie das UK die Vorteile der KI nutzen kann, ohne in die Worst-Case-Falle zu geraten – sprich, wie man sich in Richtung des Best-

Case/Balance-Szenarios bewegen kann. Diese Empfehlungen sind als **Policy-Brief** für Regierung und Parlament formuliert, mit konkreten Hebeln in den Bereichen Regulierung, Beschaffung und Governance.

10. Handlungsempfehlungen (Policy-Brief)

Abschließend werden konkrete Empfehlungen formuliert, wie Großbritannien die skizzierten Risiken abmildern und die Chancen der KI-Innovation nutzen kann, **ohne digitale Souveränität und demokratische Kontrolle zu verlieren**. Diese Empfehlungen richten sich an politische Entscheidungsträger (UK-Parlament, Regierung) und sind in kurzer Policy-Brief-Manier gehalten, gegliedert nach Handlungsfeldern: rechtlich-regulatorische Hebel, wettbewerbs- und beschaffungsbezogene Maßnahmen, Daten- und Governance-Safeguards sowie strategische Initiativen für Resilienz.

10.1 Rechtliche und regulatorische Hebel stärken

1. MoU in rechtlich bindenden Rahmen überführen: Die Freiwilligkeit des MoU sollte in einen **verbindlichen Kooperationsvertrag** übergehen. Darin klar regeln: *Datenzugriff, Haftung, Streitbeilegung*. Empfehlenswert ist die Vereinbarung spezifischer **SLAs (Service Level Agreements)** mit OpenAI für Verfügbarkeit und Performance sowie eine **Schiedsklausel** für Konflikte. So wird aus dem politischen Gentlemen's Agreement ein belastbares Vertragswerk.

2. KI-Grundsätze gesetzlich festschreiben: Das Parlament sollte einen **“AI Accountability Act”** erlassen, der für jeglichen KI-Einsatz im öffentlichen Sektor Mindeststandards vorgibt: z.B. Pflicht zur menschlichen Letztentscheidung (Kein vollautomatisierter Verwaltungsakt ohne menschliche Unterschrift), **Begründungspflicht** auch für KI-gestützte Entscheidungen und Auditierbarkeit durch unabhängige Stellen. Dieser Rahmen gilt anbieterunabhängig und stellt sicher, dass demokratische Prinzipien gewahrt bleiben, egal welcher Tech geliefert wird.

3. Datenschutz und Cloud-Regulierung anpassen: Um der CLOUD-Act Problematik zu begegnen, könnte UK gesetzlich festlegen, dass **besonders sensible Daten** nur in IT-Systemen verarbeitet werden dürfen, die unter britischem oder vergleichbarem Datenschutz stehen. Falls OpenAI-Dienste genutzt, muss *mindestens* sichergestellt sein, dass **UK Data Protection laws** gelten (z.B. via britische Cloud-Infrastruktur, siehe nächster Punkt). Zudem sollte UK bilateral mit den USA ein **Abkommen** anstreben, das den Anwendungsbereich von CLOUD Act/FISA für UK-Regierungsdaten einschränkt – analog zu

bestehenden Rechtshilfeabkommen, nur eben für Cloud-Daten (eine Herausforderung, aber im Lichte der Special Relationship einen Vorstoß wert).

4. Transparenzvorschriften verschärfen: Machen Sie den **Algorithmic Transparency Standard (ATRS)** verpflichtend für alle Behörden. Jede Nutzung von KI im Amt muss öffentlich dokumentiert werden (im Transparenzportal), inkl. Informationen über Datenquellen, Funktionsweise, Anbieter. Ergänzend richten Sie eine **parlamentarische Berichtspflicht** ein: Die Regierung soll jährlich dem zuständigen Ausschuss eine Liste aller eingesetzten KI-Systeme und Erfahrungsberichte vorlegen. Das erhöht den politischen Druck, verantwortungsvoll mit KI umzugehen, und ermöglicht parlamentarische Kontrolle.

5. Wettbewerb schützen – CMA engagieren: Bitten Sie die Wettbewerbsbehörde CMA, ein Auge auf den entstehenden KI-Markt zu haben. Falls nötig, soll CMA **Interventionen** prüfen, etwa Auflagen, dass OpenAI Schnittstellen offenlegen muss, um Konkurrenzintegration zu erleichtern (z.B. **Interoperabilitätsverpflichtungen** ähnlich wie in anderen Tech-Märkten diskutiert wird). So verhindern Sie, dass ein Anbieter alle andere verdrängt und sichern langfristig Innovationsvielfalt.

10.2 Beschaffung, Wettbewerb und Open-Source fördern

6. Multi-Anbieter-Strategie umsetzen: Vermeiden Sie ab sofort Monokulturen. Bei jeder neuen KI-Anwendung im öffentlichen Sektor soll geprüft werden, ob **ein zweiter Anbieter oder ein Open-Source-System** parallel eingesetzt werden kann (Pilot parallel laufen lassen). Zudem sollten Ausschreibungen, wo möglich, **technologieoffen** formuliert werden, nicht direkt auf OpenAI zugeschnitten. Eine **Cloud-neutral**-Policy (ähnlich Cloud First, aber neutral) könnte vorschreiben, dass möglichst keine Abhängigkeit von proprietären Features entsteht.

7. Exit-Optionen vereinbaren: Verlangen Sie in Verhandlungen mit OpenAI **Vertragsklauseln für Exit/Migration**. Beispielsweise: Datenportabilität (OpenAI muss im Falle des Vertragsende alle Rohdaten/Protokolle strukturiert zurückgeben), Unterstützung einer Übergangsphase (z.B. noch 1 Jahr Service nach Kündigung zu fairen Bedingungen), und **Know-how-Transfer** an britische Teams, damit diese notfalls Systeme eigenständig weiterbetreiben könnten. Diese Vorkehrungen mindern Lock-in.

8. Open-Source-KI als strategische Reserve fördern: Stellen Sie gezielt Fördergelder bereit (z.B. aus dem £1 Mrd Compute-Fonds), um **Open-Source-Alternativen** aufzubauen. Konkret: Finanzierung eines britischen LLM-Projekts zusammen mit Hochschulen und EU-Partnern, das mittelfristig ein Modell hervorbringt, das 80% der Behördentexte verarbeiten

kann. Auch kleinere Tools (Document-Summarizer, Chatbot-Frameworks) könnten Open-Source entwickelt werden und überall einsetzbar sein. Diese „**digitale Reservearmee**“ muss nicht immer vorn liegen, aber im Krisenfall einspringen können.

9. Heimische KI-Startups einbinden: Richten Sie ein **Public Sector AI Sandbox**-Programm ein, in dem britische Startups in Behörden Pilotprojekte durchführen dürfen – parallel zu OpenAI. Zum Beispiel: Ein Startup darf seinen spezialisierten Algorithmus 6 Monate im NHS testen, begleitet von DSIT. So geht Innovation Bottom-up. Außerdem erwägen Sie **Vorgaben bei Ausschreibungen**, einen Anteil an KMU-Beteiligung zu sichern (z.B. bei jedem großen KI-Projekt, muss es Komponenten von kleineren britischen Anbietern geben – analog zu Local Content Klauseln). Das verhindert Marktverdrängung und stärkt das Ökosystem.

10. Kostenfallen meiden – langfristige Kalkulation: Lassen Sie eine unabhängige Finanzanalyse erstellen, die **TCO (Total Cost of Ownership)** der KI-Integration über 5–10 Jahre projiziert, inkl. möglicher Gebührensteigerungen. Verankern Sie in Haushaltsplanungen einen „**digital sovereignty fund**“, aus dem Mittel bereitstehen, um im Zweifel Alternativen zu finanzieren, falls ein Anbieter überteuert wird. Dieses Polster gibt Verhandlungsmacht: OpenAI weiß dann, UK könnte Wechsel finanzieren, falls man Preise überzieht.

10.3 Datenhoheit und Sicherheit gewährleisten

11. Datenlokalisierung durchsetzen: Fordern Sie von OpenAI vertraglich, dass *sämtliche Regierungs- und Bürgerdaten in UK/EU-Rechenzentren* verarbeitet und gespeichert werden (idealerweise in Government-grade Cloud-Umgebungen). Verlangen Sie **technische Measures** wie Kundenseitige Verschlüsselung: Behörden sollen, wo machbar, Daten selbst verschlüsseln bevor sie an OpenAI-Dienste gehen, sodass OpenAI keinen Klartext sieht (außer es ist für die KI-Funktion nötig). So minimieren Sie Risiko bei US-Zugriff – selbst bei Herausgabe wären Daten unentzifferbar.

12. Britische Cloud-Infrastruktur nutzen: Nutzen Sie den Aufbau der **AI Growth Zones** gezielt: Wenn UK ohnehin £2 Mrd. investiert, koppeln Sie daran die Bedingung, dass diese Infrastruktur unter britischer Hoheit bleibt. Ideal wäre, OpenAI betreibt die KI-Modelle in einem **GBR-Cloud** (möglicherweise in Partnerschaft mit einem britischen Cloud-Anbieter oder der NHS/UKCloud Strukturen). Alternativ: Multi-Cloud-Betrieb (OpenAI auf Azure UK-Region, plus Backup auf einem UK-basierten Cloud-Anbieter wie BT oder kleinerer Provider). Das schafft Redundanz und rechtliche Handhabe, da britische Akteure involviert.

13. Cloud-Act-Schutzmechanismen einsetzen: Prüfen Sie den Abschluss eines „**UK-U.S. CLOUD Act Executive Agreement**“ spezifisch für Regierungsdaten (ähnlich wie es ein Abkommen für Strafverfolgungsbehörden gibt). Alternativ, nutzen Sie **technische/legal Workarounds**: z.B. Daten treuhänderisch von einer britischen Regierungsstelle verwalten lassen, die nur das Modell queries, aber Rohdaten nicht an OpenAI weitergibt. Solche Konstruktionen können die direkte Verfügbarkeit für US-Anordnungen erschweren.

14. Unabhängige KI-Auditoren etablieren: Richten Sie ein **AI-Oversight Board** ein (mit Vertretern von ICO, Parlamentsausschuss, Technikexperten, Zivilgesellschaft). Diese Einheit bekommt Befugnis, stichprobenartig KI-Systeme in Behörden zu prüfen, inklusive Einsicht in Modelle (notfalls im Closed Room ohne Weitergabe, um IP zu schützen). OpenAI sollte im Vertrag zustimmen, diese Prüfrechte zu gewähren. Das Board berichtet dem Parlament, ob z.B. Datenschutz eingehalten wird, ob Bias-Tests bestanden wurden etc. Dadurch wird Vertrauen aufgebaut und Missbrauch früh erkannt.

15. Notfallpläne für Ausfälle: Erarbeiten Sie für jede kritische KI-Anwendung einen **Fallback-Plan** (z.B. wenn GPT-Service 1 Woche ausfällt, wie läuft die Behörde weiter? Kann man manuell überbrücken oder auf anderes System schalten?). Schulen Sie Personal für diese Szenarien. Vereinbaren Sie mit OpenAI auch *Business Continuity*-Regelungen, etwa bevorzugter Support im Krisenfall, Zugang zu technischen Parametern falls Debugging nötig. So stellen Sie sicher, dass ein KI-Blackout nicht gleich zum Verwaltungsstillstand führt.

10.4 Demokratische Kontrolle und Werte sichern

16. Öffentlichkeitsbeteiligung und Debatte fördern: Starten Sie eine **breite öffentliche Konsultation** zum Thema “KI im öffentlichen Dienst”. Nutzen Sie dafür z.B. das Tool, das schon existiert (Consult), aber binden Sie Bürger aktiv ein. Ziel: Herausfinden, wo Akzeptanzgrenzen liegen, welche Anwendungen erwünscht oder abgelehnt werden. Diese Ergebnisse sollen transparent ausgewertet und im Parlament diskutiert werden, um dem KI-Einsatz ein *demokratisches Mandat* zu geben.

17. Ethik-Gremien in Projekte einbinden: Bei jedem größeren KI-Projekt (z.B. KI in Justiz) richten Sie einen **Ethik-Beirat** ein – interdisziplinär (Juristen, Ethiker, Bürgerrechtsvertreter). Dieser begleitet die Entwicklung und Implementierung, prüft auf Einhaltung von Grundrechten. Seine Empfehlungen sollten veröffentlicht werden. Das erhöht Legitimierung und verhindert blinde Flecken.

18. Bildung und Aufklärung der Bevölkerung: Starten Sie Kampagnen, um Bürgern **KI-Kompetenz** zu vermitteln, gerade im Umgang mit Behörden-KI. Wenn z.B. Chatbots in Ämtern antworten, klären Sie auf, dass Bürger immer noch das Recht haben, einen Menschen zu verlangen. Schulen Sie auch Richter, Beamte, damit diese KI-Ausgaben kritisch reflektieren. Ein informierter Umgang mindert das Risiko, dass KI-Fehler unbemerkt bleiben oder dass Bürger das Gefühl haben, ausgeliefert zu sein.

19. Safeguards gegen algorithmische Willkür: Implementieren Sie technisch und organisatorisch: **Bias-Tests** vor Inbetriebnahme eines KI-Systems (mit diverser Testdaten prüfen, keine Diskriminierung erkennbar). **Beschwerdewege:** Jede Person, die meint, durch eine KI-gestützte Entscheidung falsch behandelt worden zu sein, muss leicht Beschwerde einlegen können – idealerweise an eine zentrale Stelle wie den Ombudsmann. Diese Stelle braucht Zugang zur technischen Analyse (ggf. via dem KI-Oversight Board). So wird sichergestellt, dass es Korrektiv gibt, falls KI sich irgendwo unfair verhält.

20. Internationale Kooperation auf Wertebasis: Arbeiten Sie mit gleichgesinnten Ländern und Institutionen (z.B. G7, OECD) an **Standards für vertrauenswürdige KI** im Public Sector. Das UK kann hier proaktiv eine Rolle spielen und so auch OpenAI ins Boot holen, diese Standards zu erfüllen. Wenn diese z.B. einen gewissen Transparenzgrad oder Audits vorschreiben, kann UK argumentieren, man folge internationalen Best Practices (was auch OpenAI Druck macht, mitzumachen oder Risiko Imageverlust). So wird KI-Einsatz global etwas gezügelt im Sinne demokratischer Werte, was letztlich auch dem UK nutzt (vermeidet Wetttrüsteniveau, wo Ethik verloren geht).

10.5 Strategische Ausrichtung und Resilienz

21. Langfristige KI-Souveränitätsstrategie: Ergänzen Sie den AI Action Plan um ein Kapitel **“Digital Sovereignty & Resilience”**. Definieren Sie darin Ziele wie: x% der KI-Systeme sollen bis Jahr Y auf auditierbaren oder lokalen Lösungen basieren; Aufbau von n eigenen Hochsicherheits-Datacentern; Reduzierung der Abhängigkeit von einzelnen Anbietern (mit KPI, z.B. kein Anbieter >50% der kritischen KI). Monitoren Sie diese Ziele jährlich. Dies gibt klaren Kurs vor und macht Erfolg messbar (Leitfrage 1 – Metriken!).

22. Europäische Zusammenarbeit: Auch außerhalb der EU kann UK bei europäischen KI-Projekten mitmachen. Prüfen Sie den Beitritt zu Initiativen wie **CERN for AI** oder bilaterale Projekte mit Ländern wie Frankreich oder Germany, die stark in KI-Forschung investieren. Gemeinsame offene Modellprojekte könnten helfen, Alternativen zu schaffen und Abhängigkeiten von USA/China zu reduzieren. UK kann da seine exzellenten Unis einbringen. Dies diversifiziert die geopolitische Aufstellung und erhöht Resilienz.

23. Evaluierung der Partnerschaft: Setzen Sie ein fixes Datum (z.B. Ende 2026) für eine **umfassende Evaluierung** des OpenAI-MoU. Dabei sollen unabhängige Gutachter prüfen: Hat OpenAI geliefert (Investitionen, Nutzen)? Wo gab es Probleme (Datenschutz, etc.)? Das Ergebnis geht ans Parlament, das dann entscheidet, ob Auflagen verschärft oder Kurs geändert wird. Diese Klausel hält beide Seiten auf Trab: OpenAI hat Anreiz, gut zu performen (sonst droht Rückzug des UK), und die Regierung behält Möglichkeit zur Korrektur.

24. Notfallszenarien bereit halten: Seien Sie vorbereitet auf Extremfälle: Was tun, wenn OpenAI insolvent geht oder aufgrund US-Politik Dienste verlieren? → **Notfallteam** in DSIT, das Plan in der Schublade hat (z.B. schnelle Umschwenken auf Microsoft's eigen Modelle oder andere). Was tun, wenn massiver Bias-Skandal? → Mechanismus definieren (Sofort unabhängige Untersuchungskommission einsetzen, ggf. vorübergehend Nutzung aussetzen, etc.). Diese "War Games" können in Ruhe durchgespielt werden, damit im Ernstfall handlungsfähig.

25. Kommunikation der Erfolge und Grenzen: Schließlich, um Vertrauen der Bürger zu halten: Kommunizieren Sie offen sowohl **Benefits** (z.B. „Dank KI-Assistent X konnten 5 Mio Pfund eingespart und Wartezeit um 2 Wochen verkürzt werden“) als auch die **Grenzen** („KI Y wird nicht über Leben und Tod entscheiden, sondern nur Vorschläge machen.“). Diese klare Kommunikation nimmt utopische wie dystopische Missverständnisse raus. Ein realistisches Bild fördert informierte öffentliche Unterstützung.

Schlussgedanke: Mit diesen Maßnahmen kann Großbritannien den schmalen Grat meistern, **Innovationsführer** in GovTech zu sein, ohne zum **Erfüllungsgehilfen eines Tech-Monopolisten** zu werden. Es erfordert proaktive Steuerung, Transparenz und Mut zu Alternativen. Doch die Belohnung ist groß: KI kann enorme Vorteile bringen, wenn sie unter Wahrung demokratischer Werte eingesetzt wird. So kann das UK sowohl im KI-Zeitalter florieren als auch ein **Leuchtturm der digitalen Souveränität** bleiben – ein Vorbild, das zeigt, dass technischer Fortschritt und freiheitliche Kontrolle **kein Widerspruch** sein müssen^[85].

Quellen: (Aus Platzgründen im Policy-Brief nur Auswahl, vollständig im Anhang des Research Papers.)

- OpenAI/DSIT MoU Originaltext, 21. Juli 2025[1][37].
- TechPolicy Press: Kirkwood, M. „UK Deepens Dependence on US Tech...“, 24. Jul 2025[34][51].
- The Guardian: Booth, R. „UK urged to offer more transparency over OpenAI deal“, 23. Jul 2025[11][42].
- ActuIA: Benoit, M.-C. „UK–OpenAI Partner to Accelerate AI Adoption“, 25. Jul 2025[86][6].
- The Register: Halfacree, G. „UK gov swoons over OpenAI...“, 22. Jul 2025[25][19].
- Civo Blog: „Is your cloud data sovereign? CLOUD Act...“, 24. Jul 2025[49][4].

[1] [19] [25] [33] [65] [66] [68] [69] [70] UK swoons over OpenAI in legally meaningless love-in • The Register

https://www.theregister.com/2025/07/22/openai_to_help_fix_nhs/

[2] [5] [11] [42] [43] [45] [56] [61] [62] [75] [76] [78] [83] [84] UK government urged to offer more transparency over OpenAI deal | OpenAI | The Guardian

<https://www.theguardian.com/technology/2025/jul/22/uk-government-urged-to-offer-more-transparency-over-openai-deal>

[3] [4] [46] [47] [48] [49] CLOUD Act & FISA 702: Is your cloud data truly sovereign? - Civo.com

<https://www.civo.com/blog/is-your-cloud-truly-sovereign>

[6] [7] [17] [18] [20] [21] [22] [23] [24] [67] [82] [86] United Kingdom: OpenAI and DSIT Partner to Accelerate AI Adoption

<https://www.actuia.com/en/news/united-kingdom-openai-and-dsit-partner-to-accelerate-ai-adoption/>

[8] [26] [27] [71] UK and ChatGPT maker OpenAI sign new strategic partnership | Reuters

<https://www.reuters.com/world/uk/uk-chatgpt-maker-openai-sign-new-strategic-partnership-2025-07-21/>

[9] [39] [63] OpenAI signs nonbinding partnership with UK government, will explore data center investment - DCD

<https://www.datacenterdynamics.com/en/news/openai-signs-nonbinding-partnership-with-uk-government-will-explore-data-center-investment/>

[10] [13] [14] [15] [16] [29] [31] [32] [34] [36] [51] [74] [79] [80] [81] [85] UK Deepens Dependence on US Tech with New OpenAI Partnership | TechPolicy.Press

<https://www.techpolicy.press/uk-deepens-dependence-on-us-tech-with-new-openai-partnership/>

[12] [28] [35] [40] [44] Transparency tensions emerge over UK–OpenAI partnership | Capacity Media

<https://www.capacitymedia.com/article-transparency-tensions-uk-openai>

[30] [37] [38] [41] [50] [64] [72] Memorandum of Understanding between UK and OpenAI on AI opportunities - GOV.UK

<https://www.gov.uk/government/publications/memorandum-of-understanding-between-the-uk-and-openai-on-ai-opportunities/memorandum-of-understanding-between-uk-and-openai-on-ai-opportunities>

[52] [53] [54] [58] OpenAI, Google reject UK's AI copyright plan – POLITICO

<https://www.politico.eu/article/openai-google-reject-uks-ai-copyright-plan/>

[55] 'Impossible' to create AI tools like ChatGPT without copyrighted ...

<https://www.theguardian.com/technology/2024/jan/08/ai-tools-chatgpt-copyrighted-material-openai>

[57] Study claims OpenAI trains AI models on copyrighted data - AI News

<https://www.artificialintelligence-news.com/news/study-claims-openai-trains-ai-models-copyrighted-data/>

[59] [60] Algorithmic Transparency Recording Standard - guidance for public ...

<https://www.gov.uk/government/publications/guidance-for-organisations-using-the-algorithmic-transparency-recording-standard/algorithmic-transparency-recording-standard-guidance-for-public-sector-bodies>

[73] UK drops antitrust probe into Microsoft and OpenAI tie-up | Reuters

<https://www.reuters.com/technology/uk-says-microsoftopenai-partnership-does-not-need-anti-trust-investigation-2025-03-05/>

[77] UK aims to fix government IT with help from AI Humphrey • The Register

https://www.theregister.com/2025/01/21/ai_humphrey_uk_government/