GRAU DATA
Your data \ Your control _

IP-Schutz bei KI-Nutzung über den Biomed_Advisor (BmA)

📌 Ausgangslage

Die Nutzung leistungsfähiger KI-Modelle wie Claude, GPT oder Gemini ist im Forschungs- und Entwicklungsumfeld heute meist unverzichtbar.
Doch direkte Verbindungen über Browser oder Desktop-Software zu diesen Anbietern bedeuten auch direkte Verbindungen in deren Infrastrukturen – **mit gravierenden Risiken**:

- **Datenabfluss ohne Kontrolle oder Einsicht** (Prompts, Uploads, Telemetrie)
- **Fehlende Transparenz** über Speicherung, Verarbeitung oder Weitergabe
- **Rechtliche Unsicherheit** hinsichtlich geistigen Eigentums und Datenschutz

🔧 Lokale Alternativen sind derzeit keine Option

On-Premises-Lösungen erfordern hohe Investitionen, Fachpersonal, laufende Wartung und eine sehr leistungsstarke GPU-Infrastruktur – die mit der Geschwindigkeit der KI-Entwicklung kaum Schritt halten kann.
Hinzu kommt: Alle lokal betriebenen Modelle sind im biomedizinischen Kontext technologisch derzeit nicht auf dem Stand der führenden Anbieter – weder in Bezug auf Leistung, noch bei Genauigkeit, Robustheit oder Aktualität.

☑ Die Lösung

Der Biomed_Advisor (BmA) als sicherheitsfokussierte Proxy-Infrastruktur

Der Biomed_Advisor (BmA) ist eine spezialisierte KI-Plattform, die Nutzeranfragen entgegennimmt, intelligent verarbeitet und gezielt an externe Sprachmodelle weiterleitet. Dabei fungiert der BmA als technischer Proxy – ohne Inhalte zu speichern oder zu verändern. Die gesamte Plattform ist vollständig gemanagt und wird in einem renommierten deutschen Rechenzentrum betrieben – DSGVO-konform, auditierbar und unter europäischer Rechtshoheit.
Die Architektur des BmA bietet entscheidende Sicherheitsvorteile:

🔁 Der PROXY-EFFEKT

1. **Nutzer:innen kommunizieren niemals direkt mit den Modellanbietern.**
2. Der BmA übernimmt zentral die Steuerung aller Modellanfragen – ohne Session-Cookies, ohne Upload-Verläufe – und ausschließlich via API. Dabei wird der zentrale API-Key von GRAU DATA verwendet. **Für den Modellanbieter ist der Endnutzer bzw. die nutzende Organisation vollständig unsichtbar.**
3. Es gibt keine Projektordner, keine personalisierten Chatverläufe und Accounts – **der Zugriff hinterlässt keine digitalen Spuren beim Modellanbieter.**
4. **Keine Rückverfolgung, keine Transparenz für den Modellanbieter** – da die gesamte Kommunikation ausschließlich über den BmA als technischen Vermittler (Proxy) erfolgt.

🧩 Der FRAGMENTIERUNGSEFFEKT

1. **Anfragen werden gezielt auf mehrere KI-Modelle verteilt**
   → Der BmA nutzt bewusst verschiedene Sprachmodelle
   → So wird vermieden, dass Modelle vollständige Gesprächsverläufe erhalten.
2. **Auch innerhalb eines Modells erfolgt keine Weiterleitung an eine feste Instanz**
   → Der BmA setzt auf eine flexible Vermittlungsarchitektur, um Anfragen dynamisch und anonymisiert an wechselnde Modellinstanzen weiterzuleiten.
   → **Dadurch ist eine Rekonstruktion des Kontextes technisch ausgeschlossen.**
3. **Die Fragmentierung ist systemisch verankert – nicht nutzerabhängig**
   → Der Schutzmechanismus greift bei jeder einzelnen Anfrage automatisch
   → **Die Fragmentierung ist ein fest integrierter Bestandteil des Gesamtsystems.**
4. **Es entsteht kein verwertbares Nutzungsprofil bei den Modellanbietern**
   → Weder Musterbildung noch IP-Zuordnung oder organisationsbezogene Auswertung sind möglich.
   → **Die Anbieter der KI-Modelle erhalten ausschließlich isolierte, kontextlose Einzelfragmente.**

DE DEUTSCHES HOSTING

→ Der BmA wird in renommierten deutschen Rechenzentren betrieben (Hetzner o. AWS).
→ Alle Komponenten sind DSGVO-konform und unterliegen vollständig dem europäischen Datenschutzrecht.
→ Hosting, Datenverarbeitung und Zugriffspfad sind vollständig auditierbar – **für Datenschutzbeauftragte, IT-Sicherheit und Aufsichtsbehörden nachvollziehbar dokumentiert.**

🎯 FAZIT

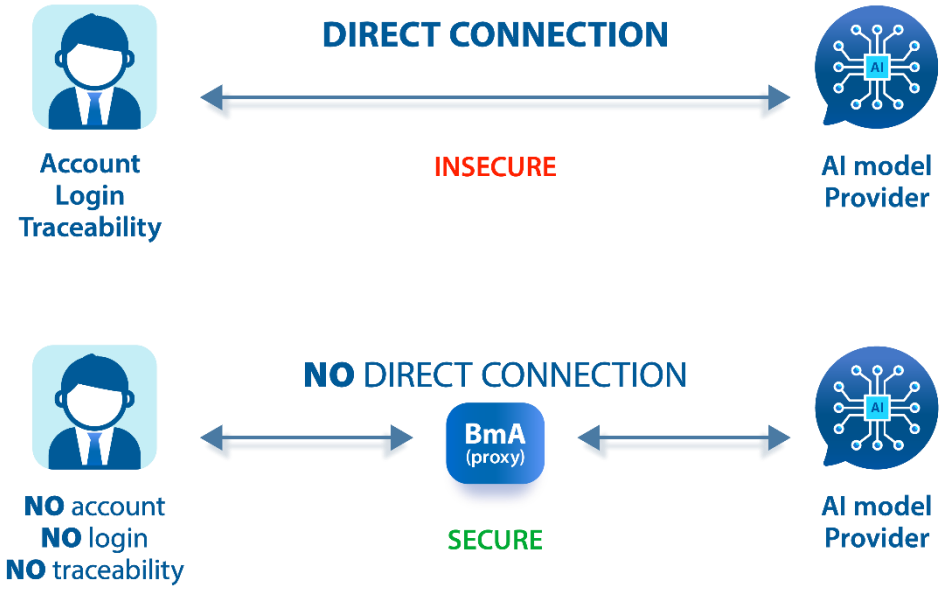
Vorteil	Wirkung
Proxy-Ebene	Trennung zwischen Nutzer:innen und Modellanbietern
Fragmentierung	Kein Modell sieht den vollständigen Inhalt
Deutsches Hosting	Kontrolle, Nachvollziehbarkeit, Datenschutz
Rechtssichere Datenhoheit	Alle Ergebnisse gehören ausschließlich der Organisation
SaaS-Lösung	Keine eigene Infrastruktur – kein Wartungsaufwand, keine Folgekosten, immer auf dem aktuellen Stand
Vertrag mit deutscher Firma	Deutscher Gerichtsstand, DSGVO-konformer Vertragspartner, keine Drittstaatenabhängigkeit

🧠 EMPFEHLUNG

Für Organisationen mit Schutzbedarf in Forschung, Entwicklung oder Verwaltung bietet der Biomed_Advisor eine technisch saubere und rechtlich abgesicherte Lösung.

Der BmA kombiniert hohe Sicherheit, minimale technische Komplexität und volle Ergebniskontrolle – ohne die Risiken direkter Modellverbindungen oder kostspieliger Inhouse-Lösungen.

PROXY-Effekt:



FRAGMENTIERUNGS-Effekt: