Ampel (Datenschutzniveau)	Form der KI-Nutzung (kurz erklärt)	Beispiele	Was ist gut möglich? (Beispiele aus der Praxis)	Was sollte nicht eingegeben werden? (Beispiele)
Dunkelrot **Sehr hohes Risiko**	**Öffentliche KI mit Privataccount** Daten werden auf Servern des Anbieters verarbeitet. Inhalte können für Produktverbesserung genutzt werden.	ChatGPT Free Gemini (privat) Claude (privat)	• Allgemeine Wissensfragen • Ideen sammeln • Texte formulieren • Fiktive Fallbeispiele erstellen • Lern- und Unterrichtsmaterial entwerfen	• Personenbezogene Daten • Reale Beratungsfälle • Gesundheitsdaten, Diagnosen • Namen, Kontaktdaten • Vertrauliche Dokumente (z. B. Berichte, Gutachten)
Orange **Erhöhtes Risiko**	**Öffentliche KI mit anonymisierten Inhalten** Wie oben, aber ohne identifizierende Angaben.	ChatGPT (privat) Gemini (privat) Claude (privat)	• Allgemeine Fallreflexion • Textentwürfe • Psychoedukation • Fiktive oder konsequent anonymisierte Beispiele	• Reale sensible Daten • Auch „anonymisierte“ Fälle, wenn Personen durch Kombination von Details wiedererkennbar sind
Dunkelgelb **Mittleres Risiko**	**Business-/Enterprise-KI** Nutzung über einen Organisationsaccount mit vertraglicher Regelung. Inhalte werden in der Regel nicht zum Modelltraining genutzt (abhängig vom Anbieter).	ChatGPT Business / Enterprise Microsoft Copilot (für Organisationen)	• Berufliche Textarbeit • Zusammenfassungen • Interne Dokumente (je nach Vertrag) • Entwürfe und Analysen • Unterstützung in Organisation und Verwaltung	• Sensible personenbezogene Daten nicht automatisch eingeben • AVV, Speicherort, Retention, Zugriffsrechte und eingesetzte Funktionen müssen geprüft sein
Hellgelb **Geringeres Risiko**	**Datenschutzorientierter KI-Zugang / Wrapper** Kontrollierte Plattform mit europäischer Infrastruktur (je nach Anbieter).	**Langdock** **MeinGPT** **9brains**	• Verschiedene KI-Modelle über eine geschützte Oberfläche • Interne Dokumente (je nach Vertrag) • Unterstützung in Beratung, Bildung und Verwaltung	• Nicht automatisch alle Daten zulässig • Datenweg des jeweils verwendeten Modells prüfen (einzelne Modelle können außerhalb der EU verarbeitet werden) • Berufsgeheimnis und Rechtsgrundlage beachten
Grün **Geringes Risiko**	**Souverän gehostete KI** KI-Modelle auf Infrastruktur in Deutschland / EU, mit klaren Datenschutzgarantien (z. B. Zero Retention).	**franconia.ai** **mittwald** **IONOS**	• Professionelle Anwendungen mit stärker kontrolliertem Datenweg • Interne Dokumente • Eigene Wissensdatenbanken (RAG) • Transkription, Analyse und Textbearbeitung	• Personenbezogene Daten nur, wenn Rechtsgrundlage, AVV und Berechtigungskonzept passen • Trotzdem Datenschutz, Berufsgeheimnis und organisatorische Schutzmaßnahmen beachten
Dunkelgrün **Eigene Infrastruktur**	**Eigene / lokale KI** KI-Modell auf eigenem Gerät oder Server (On-Premise). Daten bleiben bei Ihnen.	Ollama LM Studio Jan (lokal) Eigener Server /	• Lokale Dokumentenanalyse • Eigene Wissensbestände durchsuchen • Textbearbeitung • Eigene Anwendungen entwickeln • Vollständig offline möglich	• Vorsicht bei Websuche, externen APIs oder Plugins – sie können Daten nach außen übertragen • Cloud-Synchronisation deaktivieren • Zugriffsschutz, Updates, Logging- und Löschkonzepte umsetzen

Ampelfarbe = Kontrolle über den Datenweg, nicht die Qualität der KI. | Auch bei „grünen“ Lösungen gelten Datenschutz, Berufsgeheimnis, Zugriffsschutz und Zweckbindung.

Medieninhaber und Herausgeber: Forschungsgreisslerei –
Verein zur Förderung von Wissenschaft und Forschung