Datenschutz & digitale Souveränität bei KI-Chatbot-Systemen

Diese Handreichung bietet eine verständliche Orientierung und ersetzt keine Rechtsberatung. Für konkrete Projekte sollten die zuständige Datenschutzaufsichtsbehörde und die behördliche Datenschutzbeauftragte frühzeitig einbezogen werden.

Im Mittelpunkt steht, wie öffentliche Stellen bei KI-Chatbot-Systemen die Kontrolle über Daten behalten, sichere Architekturen gestalten und Berührungspunkte zum EU-AI-Act beachten. Die Ausführungen basieren auf einer Masterarbeit mit Schwerpunkt auf Retrieval-Augmented Generation (RAG), gelten jedoch weitgehend für KI-Chatbot-Systeme im öffentlichen Sektor allgemein.

💡 Leitgedanke für den Start

Datenschutz als Ermöglicher, nicht als Blockierer: Datenschutz sollte Innovation nicht blockieren, sondern verantwortliches Handeln ermöglichen. [1]

Experimentierräume nutzen: Erste Tests in sicherem, kleinem Rahmen durchführen, um Erfahrungen zu sammeln und Vertrauen aufzubauen. [2]

Pragmatischer Einstieg: Mit nicht personenbezogenen Daten testen, Datenschutzprüfungen schrittweise vertiefen. [3], [2]

Zweck als Kompass: Verarbeitung muss spezifisch, explizit und legitim sein; Zweck vorab festlegen. [4], [5]

1 Phase 1: Grundlagen schaffen und Zielbild klären

- **KI-Chatbot-Systeme verstehen:** KI-Chatbots verarbeiten Eingaben und generieren Antworten. Bei RAG-Systemen werden zusätzlich relevante Textpassagen aus Wissensquellen abgerufen und in den Prompt integriert. [6], [7]
- **Qualität der Antworten sicherstellen:** Auch bei RAG-Systemen können fehlerhafte Inhalte entstehen. Qualitätskontrollen und menschliche Überprüfung bleiben wichtig. [8], [6]
- **Zieldefinition klären:** Welche Aufgaben soll das System unterstützen? Welche Datenkategorien sind betroffen? Datenschutz ist stark kontextbezogen. [9]
- **Datenminimierung sicherstellen:** Verarbeitung personenbezogener Daten vermeiden, wenn für den Anwendungsfall nicht erforderlich. Nur die Daten verarbeiten, die für die Erfüllung der Aufgabe unbedingt nötig sind. [5], [3]

- **Personenbezug prüfen:** Wenn das System keine personenbezogenen Daten als Eingabe erhält und nicht mit solchen arbeitet, greift die DSGVO nicht. Dies sollte in den Nutzungsbedingungen klargestellt werden. Früh prüfen, ob in Dokumenten oder Logs personenbezogene Daten vorkommen könnten. [3]

Wenn das Zielbild steht, rückt als nächster Schritt die Datenbasis in den Fokus.

2 Phase 2: Datenbasis, Datenqualität und Urheberrecht

- **Datenkategorien unterscheiden:** Öffentliche vs. interne Daten. Öffentliche Zugänglichkeit hebt Schutz personenbezogener Daten nicht auf. [10], [9]
- **Datenqualität sichern:** Vollständigkeit, Genauigkeit, Konsistenz und Aktualität bestimmen Zuverlässigkeit der Antworten. [11], [9]
- **Datenpflege kontinuierlich gestalten:** Löschfristen, Aktualisierungen und nachvollziehbare Review-Prozesse etablieren. [12], [3]

Kurzer Seitenblick: Urheberrecht

Externe Webinhalte: Nutzung kann urheberrechtlich relevant sein, besonders bei langfristiger Speicherung oder Reproduktion. [13], [14]
Text- und Data-Mining: In EU grundsätzlich erlaubt, aber nur wenn Rechteinhaber kein wirksames Opt-out erklärt haben und Nutzung zeitlich begrenzt bleibt. [15], [14]

Sind Datenbasis und Rechtefragen geklärt, folgt die architektonische Umsetzung.

3 Phase 3: Prototyping, Architektur und digitale Souveränität

- **Schnittstellen prüfen:** Vorhandene oder veraltete Schnittstellen identifizieren und bei Bedarf aktualisieren oder neu entwickeln. [16]
- **Abhängigkeiten managen:** Bei RAG-Systemen kann der Wechsel des Embedding-Modells eine Neu-Indexierung der Wissensbasis erfordern. Modularität und Austauschbarkeit der Komponenten beachten. [17], [6]
- **Digitale Souveränität sichern:** Datenflüsse und Technologiezugänge kontrollierbar gestalten; staatliche Steuerungsfähigkeit und individuelle Kontrolle ermöglichen. [18], [19]
- **Open-Source-Optionen bewerten:** Open-Source-Komponenten können Abhängigkeiten reduzieren, erfordern aber klare Qualitäts- und Sicherheitsverantwortung. [20], [2]

4 Phase 4: Compliance, Sicherheit und AI-Act-Berührungspunkte

Rechtsgrundlagen, Zweckbindung und Transparenz

Rechtsgrundlage prüfen: Für öffentliche Stellen ist bei öffentlichen Daten oft die Wahrnehmung öffentlicher Aufgaben möglich. Andernfalls ist eine Einwilligung erforderlich (berechtigtes Interesse reicht nicht). [21], [9]

Zweckbindung festlegen: Verarbeitungszweck vorab präzise definieren; Zweckänderungen gesondert prüfen. [4], [5]

Transparenz gewährleisten: Verständliche Informationen über Zwecke, Rechtsgrundlagen, Empfänger und Speicherdauer bereitstellen. [22], [23]

Rollen, Verantwortlichkeiten und Dokumentation

Rollen klar definieren: Verantwortlicher und Auftragsverarbeiter vertraglich fixieren; Verantwortung bleibt bei der verantwortlichen Stelle. [3]

Dokumentation sicherstellen: Nachvollziehbare Dokumentation führen, Verzeichnis von Verarbeitungstätigkeiten pflegen, Kontrollen protokollieren. [24], [25]

Datenschutz-Folgenabschätzung (DSFA)

Bei hohen Risiken durchführen: Systematische Identifikation, Bewertung und Minderung von Risiken; frühzeitig ansetzen. [25], [26]

Technische und organisatorische Maßnahmen (TOM)

Privacy by Design/Default umsetzen: Zugriffskontrollen, Pseudonymisierung, Verschlüsselung, Monitoring implementieren. [27], [24]

Sicherheitsmaßnahmen etablieren: Input-Filter, Rollen-/Rechtekonzepte, Sicherheitstests einrichten. [28]

Datenschutzprüfung bei der Eingabe: Automatische Erkennung und Maskierung personenbezogener Daten (Namen, Gesundheits- oder Finanzdaten) in Eingaben implementieren; Warnhinweise im Chatfenster anzeigen. [29], [30]

AI Act: Risikoklassen, Transparenz und Kompetenz

Risikobasierte Einordnung vornehmen: Chatbots meist „begrenztes Risiko" mit Transparenzpflichten. [31], [32]

KI-Kompetenz aufbauen: Angemessene Kompetenz des Personals je nach Einsatzkontext sicherstellen. [33], [12]

Drittlandtransfers und souveräne Datenflüsse

DSGVO-Voraussetzungen einhalten: Angemessenes Datenschutzniveau oder geeignete Garantien sicherstellen. [3]

EU-US Data Privacy Framework nutzen: Erleichtert Transfers in USA, bleibt aber rechtlich sensibel. [34], [35]

Standardvertragsklauseln anwenden: Transfer-Folgenabschätzung durchführen und zusätzliche Schutzmaßnahmen implementieren. [36], [3]

5 Phase 5: Rollout, Befähigung und dauerhafte Akzeptanz

Nach den rechtlichen und technischen Aspekten folgt die organisatorische Umsetzung.

- **Nutzen sichtbar machen:** Akzeptanz hängt stark von sichtbar erzieltem Nutzen ab. Kompetenzaufbau und klare Zuständigkeiten fördern die Nutzung. [16], [37]
- **Change-Management und Schulungen:** Vertrauen aufbauen und Qualität der Antworten fortlaufend verbessern. [2], [11]

✓ Abschluss: Worauf es ankommt

- **Ganzheitlicher Ansatz:** KI-Chatbot-Systeme erfordern ein Zusammenspiel aus Recht, Daten-Governance, Architektur und Organisation über den gesamten Lebenszyklus. [38]
- **Verzahnung als Schlüssel:** Datenschutzkonforme Systeme sind erreichbar, wenn Zweck, Rechtsgrundlage, Datenqualität, Sicherheitsarchitektur, Verantwortlichkeiten und Kompetenzaufbau von Anfang an verzahnt werden. [25], [12]
- **Kontrolle als Souveränität:** Digitale Souveränität bedeutet, Datenflüsse, Anbieter und Wissen dauerhaft kontrollieren zu können. [18], [2]

? Unterstützung und weiterführende Ressourcen

Interne Ansprechpersonen

Datenschutzbeauftragte/r einbinden: Frühzeitig bei der Planung neuer KI-Chatbot-Systeme, bei der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten und bei der Prüfung, ob eine DSFA erforderlich ist. [12]

Informationssicherheitsbeauftragte/r und IT-Fachbereich: Für technische Sicherheitsaspekte und Architekturentscheidungen. [28]

Externe Orientierungshilfen und Aufsichtsbehörden

Datenschutzkonferenz (DSK): Orientierungshilfe „Künstliche Intelligenz und Datenschutz" (2024) und spezifische Orientierungshilfe zu KI-Systemen mit Retrieval Augmented Generation (RAG) (2025). [39], [40]

Landesdatenschutzbehörden: Informationsangebote und Leitfäden zum Thema KI und Chatbots (z.B. LfD Niedersachsen, LDA Bayern, BfDI). [41]

European Data Protection Board (EDPB): Guidelines und Berichte zu KI-Systemen, z.B. ChatGPT-Taskforce-Report. [42]

Weitere Leitfäden und Ressourcen

Bitkom-Leitfaden: „KI und Datenschutz – Praxisleitfaden für Unternehmen" (2024). [43]
Positionspapier der DSK: „Empfohlene technische und organisatorische Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen" (2019). [44]

Rechtliche und fachliche Beratung

Externe Expertise: Bei komplexen Vorhaben, sensiblen Datenkategorien oder DSFA-Pflicht kann externe rechtliche Beratung (Schwerpunkt Datenschutzrecht) sowie technische Expertise im Bereich KI-Sicherheit sinnvoll sein. [25]
Kontakt zu Aufsichtsbehörden: Bei spezifischen Fragen oder Unsicherheiten frühzeitig Kontakt aufnehmen, um datenschutzrechtliche Anforderungen im Vorfeld zu klären. [3]

Die vollständige Masterarbeit herunterladen

Die Masterarbeit „Zentrale Herausforderungen bei der datenschutzkonformen Umsetzung eines RAG-KI-Chatbots für öffentliche Stellen" von Marvin Prigenitz (2025) kann hier heruntergeladen werden:

https://innowest-brandenburg.de/publikationen

Quellenverzeichnis

- **[1]** Fahimi, Y., Kelber, U., & Kramarsch, M. (2023). Digitale Ethik 5: Yasmin Fahimi und Ulrich Kelber. https://demographienetzwerk.de/mediathek/artikel/impulsreihe-digitale-ethik/digitale-ethik-5-yasminfahimi-und-ulrich-kelber/
- **[2]** Bharosa, N., & Janowski, T. (2024). The GovTech Challenge – GovTech and Public Value Creation. Proceedings of the 25th Annual International Conference on Digital Government Research, 1043–1045. https://doi.org/10.1145/3657054.3659125
- **[3]** Voigt, P., & Von Dem Bussche, A. (2024). EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch. Springer. https://doi.org/10.1007/978-3-662-68820-5
- **[4]** Klenk, T., Nullmeier, F., & Wewer, G. (Hrsg.). (2025). Handbuch Digitalisierung in Staat und Verwaltung. Springer Fachmedien. https://doi.org/10.1007/978-3-658-37373-3
- **[5]** Kugelmann, D. (2024). Scharniere zwischen DS-GVO und KI. Datenschutz und Datensicherheit - DuD, 48(8), 496–502. https://doi.org/10.1007/s11623-024-1966-2
- **[6]** Gao, Y., Xiong, Y., Gao, X., Jia, K., Pan, J., Bi, Y., Dai, Y., Sun, J., Wang, M., & Wang, H. (2024). Retrieval-Augmented Generation for Large Language Models: A Survey (No. arXiv:2312.10997). arXiv. https://doi.org/10.48550/arXiv.2312.10997

- **[7]** Swacha, J., & Gracel, M. (2025). Retrieval-Augmented Generation (RAG) Chatbots for Education: A Survey of Applications. Applied Sciences, 15(8). https://doi.org/10.3390/app15084234
- **[8]** Leible, S., Gücük, G.-L., Simic, D., von Brackel-Schmidt, C., & Lewandowski, T. (2024). Zwischen Forschung und Praxis: Fähigkeiten und Limitationen generativer KI sowie ihre wachsende Bedeutung in der Zukunft. HMD Praxis der Wirtschaftsinformatik, 61(2), 344–370. https://doi.org/10.1365/s40702-024-01050-x
- **[9]** Ruschemeier, H. (2025). LLMs und Datenschutzrecht. Datenschutz und Datensicherheit - DuD, 49(6), 349–354. https://doi.org/10.1007/s11623-025-2102-7
- **[10]** von Lucke, J., & Etscheid, J. (2020). Künstliche Intelligenz im öffentlichen Sektor. HMD Praxis der Wirtschaftsinformatik, 57(1), 60–76. https://doi.org/10.1365/s40702-019-00579-6
- **[11]** Schmidt, M. (2024). Einsatz von künstlicher Intelligenz für sachbearbeitende Tätigkeiten im öffentlichen Dienst. Wirtschaftsinformatik & Management, 16(2), 123–132. https://doi.org/10.1365/s35764-024-00516-3
- **[12]** Venzke-Caprarese, S. (2025). Interne Regelungen zum Einsatz von Künstlicher Intelligenz. Datenschutz und Datensicherheit - DuD, 49(6), 396–401. https://doi.org/10.1007/s11623-025-2110-7
- **[13]** Desai, D. R., & Riedl, M. (2024). Between Copyright and Computer Science: The Law and Ethics of Generative AI (No. arXiv:2403.14653). arXiv. https://doi.org/10.48550/arXiv.2403.14653
- **[14]** Novelli, C., Casolari, F., Hacker, P., Spedicato, G., & Floridi, L. (2024). Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity (No. arXiv:2401.07348). arXiv. https://doi.org/10.48550/arXiv.2401.07348
- **[15]** Lucchi, N. (2024). ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems. European Journal of Risk Regulation, 15(3), 602–624. https://doi.org/10.1017/err.2023.59
- **[16]** Degen, T. A., & Waitzinger, S. (2025). KI-Projekte datenschutzkonform planen und kontrollieren—KI-Einsatz bei Behörden, kritischer Infrastruktur und Unternehmen. Ausbildung - Prüfung - Fachpraxis (APF), 4, 109–114.
- **[17]** Gao, Y., Xiong, Y., Wang, M., & Wang, H. (2024). Modular RAG: Transforming RAG Systems into LEGO-like Reconfigurable Frameworks (No. arXiv:2407.21059). arXiv. https://doi.org/10.48550/arXiv.2407.21059
- **[18]** Chander, A., & Sun, H. (Hrsg.). (2023). Data Sovereignty: From the Digital Silk Road to the Return of the State. Oxford University Press. https://doi.org/10.1093/oso/9780197582794.001.0001
- **[19]** Nanni, R., Bizzaro, P. G., & Napolitano, M. (2024). The false promise of individual digital sovereignty in Europe: Comparing artificial intelligence and data regulations in China and the European Union. Policy & Internet, 16(4), 711–726. https://doi.org/10.1002/poi3.424
- **[20]** Sonabend, R., Gruson, H., Wolansky, L., Kiragga, A., & Katz, D. S. (2024). FAIR-USE4os: Guidelines for creating impactful open-source software. PLOS Computational Biology, 20(5), e1012045. https://doi.org/10.1371/journal.pcbi.1012045
- **[21]** Pesch, P. J., & Magnussen, K. (2025). LLMs im Forschungsdatenschutz. Datenschutz und Datensicherheit - DuD, 49(6), 367–372. https://doi.org/10.1007/s11623-025-2105-4

- **[22]** Bortnikov, V. (2025). Transparenz bei KI-Systemen. Datenschutz und Datensicherheit - DuD, 49(5), 297–301. https://doi.org/10.1007/s11623-025-2091-6
- **[23]** Haftenberger, A., & Dierks, C. (2023). Rechtliche Einordnung von künstlicher Intelligenz in der Inneren Medizin. Die Innere Medizin, 64(11), 1044–1050. https://doi.org/10.1007/s00108-023-01598-8
- **[24]** Feretzakis, G., Papaspyridis, K., Gkoulalas-Divanis, A., & Verykios, V. S. (2024). Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review. Information (2078-2489), 15(11), 697. https://doi.org/10.3390/info15110697
- **[25]** Hense, P., & Wagner, D. (2025). Die datenschutzrechtliche Due Diligence für KI-Systeme. Datenschutz und Datensicherheit - DuD, 49(6), 373–378. https://doi.org/10.1007/s11623-025-2106-3
- **[26]** Pfaffinger, M. (2025). Datenschutzrechtliche Fragen beim KI-Einsatz aus Schweizer Sicht. Datenschutz und Datensicherheit - DuD, 49(6), 361–366. https://doi.org/10.1007/s11623-025-2104-5
- **[27]** Ufert, F. (2020). AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI? https://doi.org/10.15166/2499-8249/394
- **[28]** Derner, E., Batistič, K., Zahálka, J., & Babuška, R. (2024). A Security Risk Taxonomy for Prompt-Based Interaction With Large Language Models. IEEE Access, 12, 126176–126187. https://doi.org/10.1109/ACCESS.2024.3450388
- **[29]** Chen, C., Zhou, D., Ye, Y., Li, T. J.-J., & Yao, Y. (2025). CLEAR: Towards Contextual LLM-Empowered Privacy Policy Analysis and Risk Generation for Large Language Model Applications. Proceedings of the 30th International Conference on Intelligent User Interfaces, 277–297. https://doi.org/10.1145/3708359.3712156
- **[30]** Zhou, J., Xu, E., Wu, Y., & Li, T. (2025). Rescriber: Smaller-LLM-Powered User-Led Data Minimization for LLM-Based Chatbots. Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3706598.3713701
- **[31]** Regulation (EU) 2024/1689. (2024, Juli). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. Official Journal of the European Union, L 1689, 1–144. http://data.europa.eu/eli/reg/2024/1689/oj
- **[32]** Ioannidou, E., Promikyridis, R., & Tambouris, E. (2025). Legal and Ethical Issues Arising from the Use of Chatbots in Public Administration. Proceedings of the 28th Pan-Hellenic Conference on Progress in Computing and Informatics, 211–215. https://doi.org/10.1145/3716554.3716586
- **[33]** Bausewein, C. (2025). Synergiepotenziale zwischen DSGVO und KI-VO für KI-System-Betreiber. Datenschutz und Datensicherheit - DuD, 49(5), 293–296. https://doi.org/10.1007/s11623-025-2090-7
- **[34]** Tschider, C., Compagnucci, M. C., & Minssen, T. (2024). The new EU–US data protection framework's implications for healthcare. Journal of Law & the Biosciences, 11(2), 1–25. https://doi.org/10.1093/jlb/lsae022

- **[35]** Lalova-Spinks, T., Valcke, P., Ioannidis, J. P. A., & Huys, I. (2024). EU-US data transfers: An enduring challenge for health research collaborations. NPJ Digital Medicine, 7(1), 1–5. https://doi.org/10.1038/s41746-024-01205-6
- **[36]** Nash, I., Kennedy-Mayo, D., Swire, P., & Antón, A. (2024). Legal Issues in Reconciling Data Protection, AI, and Cybersecurity under EU Law. Missouri Law Review, 89(3), 1–69.
- **[37]** Wielgosch, J., & Dieke, A. K. (2024). KI in Kommunen: Anwendungen, Potenziale und Hindernisse [Kurzstudie]. WIK GmbH. https://www.wik.org/veroeffentlichungen/veroeffentlichung/ki-in-kommunen-anwendungen-potenziale-und-hindernisse
- **[38]** Prigenitz, M. (2025). Zentrale Herausforderungen bei der datenschutzkonformen Umsetzung eines RAG-KI-Chatbots für öffentliche Stellen. Masterarbeit, Technische Hochschule Brandenburg.
- **[39]** Datenschutzkonferenz. (2024, Mai 6). Künstliche Intelligenz und Datenschutz: Orientierungshilfe. https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf
- **[40]** Datenschutzkonferenz. (2025). Orientierungshilfe zu KI-Systemen mit Retrieval Augmented Generation (RAG). https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_RAG.pdf
- **[41]** Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. (2025). Künstliche Intelligenz. https://www.bfdi.bund.de/DE/themen/ki-node.html
- **[42]** European Data Protection Board. (2024). Report of the work undertaken by the ChatGPT Taskforce. https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf
- **[43]** Bitkom e.V. (2024). Leitfaden KI und Datenschutz – Praxisleitfaden für Unternehmen. https://www.bitkom.org/sites/main/files/2024-07/202407bitkom-leitfaden-ki-datenschutz.pdf
- **[44]** Datenschutzkonferenz. (2019). Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen. https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf