

Herausgeber: Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V.
Titel: Vom Second Brain zum LLM-Wiki - Wissensinfrastruktur für Mitarbeitende in Compliance-Abteilungen am Beispiel der Arbeit von Datenschutzbeauftragten
Autor: Stephan Rehfeld
Datum: 17. August 2026
Kontakt: geschaeftsstelle@zki.de

Vom Second Brain zum LLM-Wiki - Wissensinfrastruktur für Mitarbeitende in Compliance-Abteilungen am Beispiel der Arbeit von Datenschutzbeauftragten

Einleitung

Datenschutzbeauftragte beraten häufig zu wiederkehrenden Fragestellungen, müssen frühere Bewertungen berücksichtigen und zugleich auf neue Rechtsentwicklungen reagieren. Das dafür benötigte Wissen liegt jedoch häufig verteilt in E-Mails, Stellungnahmen, Datenschutz-Folgenabschätzungen, Vertragsprüfungen, Präsentationen und persönlichen Notizen. Ein LLM-Wiki soll daraus eine strukturierte Wissensbasis machen, die sowohl von Menschen als auch von Sprachmodellen genutzt und weiterentwickelt werden kann. Der Beitrag erläutert das Konzept, grenzt es von Retrieval-Augmented Generation und einem Second Brain ab und zeigt anhand eines Datenschutz-Wikis, wo der praktische Nutzen, aber auch die derzeitigen Grenzen für Datenschutzbeauftragte, -auditoren, -koordinatoren und -berater liegen.

Abgrenzung des Beitrags

Gegenstand dieses Beitrags sind die Organisation von Wissen und die damit verbundenen datenschutzrechtlichen und organisatorischen Governance-Fragen. Fragen der Informationssicherheit, insbesondere die technische Absicherung der Systeme, Systemhärtung, Angriffsszenarien und die sichere technische Implementierung, werden nicht behandelt. Soweit Berechtigungen oder Vertraulichkeitsklassen angesprochen werden, geschieht dies ausschließlich aus der Perspektive der Wissens- und Nutzungs-Governance.

1 Datenschutzberatung ist auch Wissensmanagement

Datenschutzbeauftragte beantworten nur selten eine Frage, die mit keiner früheren Beratung vergleichbar ist. Ob Beschäftigtendaten in einem KI-System verarbeitet werden dürfen, wann eine Datenschutz-Folgenabschätzung erforderlich ist, welche Anforderungen an eine Auftragsverarbeitung zu stellen sind oder wie lange Forschungsdaten gespeichert werden dürfen: Die Sachverhalte unterscheiden sich, die zugrunde liegenden Bewertungsmuster wiederholen sich jedoch.

Dabei entsteht wertvolles Wissen. Es umfasst nicht nur Rechtsnormen, Urteile und Veröffentlichungen von Aufsichtsbehörden. Hinzu kommen organisationsspezifische Zuständigkeiten, interne Richtlinien, frühere Entscheidungen, dokumentierte Risiken, bewährte Maßnahmen und Erfahrungen mit bestimmten Verarbeitungssituationen. Ein erheblicher Teil dieses Wissens bleibt fallgebunden. Die fertige Stellungnahme wird abgelegt, die E-Mail archiviert und der Chat geschlossen. Bei der nächsten ähnlichen Frage beginnt die Arbeit erneut mit der Suche nach Quellen und früheren Arbeitsergebnissen.

Klassische Dokumentenablagen lösen dieses Problem nur teilweise. Sie speichern Dokumente, machen aber nicht ohne Weiteres sichtbar, welche Bewertungslinie aus mehreren Dokumenten folgt,

welche Aussage überholt ist oder welche frühere Beratung auf einen neuen Fall übertragen werden kann. Auch ein allgemeines Large Language Model (LLM) schließt diese Lücke nicht. Es kann Texte strukturieren und bekannte Rechtsfragen erläutern, kennt aber weder die Organisation noch deren bisherige Bewertungspraxis. Ohne zusätzliche Wissensbasis bleibt es ein allgemeiner Assistent.

Das LLM-Wiki setzt an dieser Stelle an. Es soll nicht lediglich weitere Dateien aufnehmen, sondern Quellen, Erkenntnisse und Arbeitsergebnisse so ordnen, dass sie dauerhaft auffindbar, miteinander verknüpft und für neue Fragestellungen wiederverwendbar werden. Die entscheidende Frage lautet daher nicht: „Welches LLM beantwortet eine einzelne Frage am besten?“ Sie lautet: „Wie organisieren wir unser Wissen so, dass Menschen und LLMs damit nachvollziehbar und kontrolliert arbeiten können?“

2 Vier Begriffe mit unterschiedlichen Funktionen

Die Diskussion wird dadurch erschwert, dass LLM-Wiki, RAG, AI Harness und Second Brain teilweise wie austauschbare Begriffe verwendet werden. Tatsächlich bezeichnen sie unterschiedliche Ebenen der Wissensarbeit.

2.1 LLM-Wiki

Ein **LLM-Wiki** ist eine strukturierte, fortlaufend gepflegte Wissensbasis, meist in Markdown, die von Menschen kuratiert und von einem LLM unterstützt erstellt, aktualisiert, verlinkt und ausgewertet wird. Anders als eine bloße Dateiablage enthält sie nicht nur Quellen, sondern verdichtetes, thematisch geordnetes und wiederverwendbares Wissen. Ziel ist eine gemeinsame, nachvollziehbare Wissensschicht für Mensch und LLM.

2.2 Retrieval-Augmented Generation

Retrieval-Augmented Generation (RAG) ist ein technisches Verfahren, bei dem ein LLM zur Beantwortung einer Anfrage relevante Inhalte aus externen Quellen sucht, als zusätzlichen Kontext erhält und daraus eine Antwort erzeugt. RAG organisiert das gefundene Wissen nicht zwingend dauerhaft, sondern stellt es für eine konkrete Anfrage bereit. Die Qualität hängt unter anderem davon ab, welche Dokumente durchsucht, wie diese aufgeteilt und indexiert, welche Textstellen gefunden und wie sie dem Modell präsentiert werden.¹

2.3 AI Harness

Ein **AI Harness** ist die kontrollierte Arbeitsumgebung um ein oder mehrere KI-Modelle. Er verbindet das Modell mit Dateien, Wissensquellen, Werkzeugen, Arbeitsabläufen, Speicherfunktionen, Berechtigungen, Protokollierung und Review-Prozessen. Der Begriff ist nicht normiert und wird am Markt uneinheitlich verwendet. In diesem Beitrag dient er als funktionaler Sammelbegriff für die Umgebung, die aus einem Sprachmodell ein arbeitsfähiges System macht.

2.4 Second Brain

Ein **Second Brain** ist ein persönliches oder teambezogenes System zur dauerhaften Organisation von Wissen, Gedanken, Quellen, Notizen und Arbeitsergebnissen. Es soll Wissen außerhalb des eigenen Gedächtnisses auffindbar und wiederverwendbar machen. Das Konzept ist nicht auf LLMs beschränkt und muss weder maschinenlesbar strukturiert noch für eine automatisierte Pflege ausgelegt sein.²

Die vier Begriffe lassen sich deshalb wie folgt zusammenführen: Das Second Brain beschreibt das übergeordnete Konzept einer externen Wissensorganisation. Das LLM-Wiki bildet eine strukturierte

¹ Patrick Lewis u. a., „Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks“, 2020, <https://arxiv.org/abs/2005.11401>.

² Vgl. Tiago Forte, *Building a Second Brain*, New York 2022. Die im Beitrag verwendete Definition ist eine auf den behandelten Kontext zugeschnittene Arbeitsdefinition.

und LLM-nutzbare Wissensschicht. RAG beschafft für eine konkrete Anfrage zusätzliche Quellen. Der AI Harness verbindet Wissen, Modell, Werkzeuge und Arbeitsabläufe.

3 Die Idee des LLM-Wikis

Der konkrete Referenzpunkt des hier behandelten Konzepts ist ein im April 2026 veröffentlichter Gist von Andrej Karpathy. Er bezeichnet das LLM-Wiki als Muster für den Aufbau persönlicher Wissensbasen mit LLMs. Das Dokument ist ausdrücklich als „idea file“ angelegt: Es beschreibt kein fertiges Produkt, sondern soll einem LLM-Agenten als konzeptionelle Arbeitsanweisung übergeben werden.³

Karpathys Ausgangskritik richtet sich gegen eine ausschließlich anfragebezogene Arbeit mit Dokumenten. Bei einem einfachen RAG-Ansatz werden zu jeder Frage passende Ausschnitte aus Rohdokumenten gesucht. Das Modell muss den Zusammenhang immer wieder neu herstellen. Eine aufwendige Synthese aus mehreren Quellen verschwindet nach der Antwort häufig im Chatverlauf. Das System findet bei der nächsten Frage möglicherweise dieselben Quellen, baut aber nicht notwendig auf der bereits geleisteten Einordnung auf.

Das LLM-Wiki soll Wissen stattdessen kumulieren lassen. Neue Quellen werden nicht nur indexiert, sondern ausgewertet und in eine bestehende Wissensstruktur eingearbeitet. Begriffsseiten werden ergänzt, Entitäten aktualisiert, Querverbindungen gesetzt und Widersprüche gekennzeichnet. Eine gute Antwort kann nach menschlicher Prüfung selbst wieder in das Wiki zurückfließen. Die Wissensbasis wächst damit nicht nur quantitativ, sondern soll über die Zeit fachlich dichter werden.

Karpathy unterscheidet drei Schichten:

1. **Rohquellen:** Die unveränderten Ausgangsmaterialien, etwa Leitlinien, Urteile, Fachaufsätze, Richtlinien, Verträge oder eigene Notizen.
2. **Wiki:** Verdichtete Markdown-Seiten, beispielsweise zu Begriffen, Organisationen, Rechtsfragen, Quellen, Vergleichen und Synthesen.
3. **Schema:** Regeln, nach denen der Agent das Wiki aufbaut und pflegt. Dazu gehören Seitentypen, Benennungskonventionen, Zitierregeln und Arbeitsabläufe.

Darauf bauen drei zentrale Vorgänge auf. Beim **Ingest** wird eine neue Quelle analysiert und in das Wiki eingearbeitet. Bei einer **Query** beantwortet das System eine Frage anhand der Wiki-Inhalte und gegebenenfalls weiterer Quellen. Beim **Lint** wird die Wissensbasis auf Widersprüche, veraltete Aussagen, fehlende Links, Dubletten und offene Wissenslücken geprüft. Eine index.md dient als fachliche Navigationskarte, eine log.md als chronologische Bearbeitungsspur.

Dieses Muster ist für die Datenschutzpraxis interessant, weil es Quelle, fachliche Verdichtung und Arbeitsregeln grundsätzlich voneinander trennt. Es zwingt allerdings noch nicht zu einer rechtlich oder organisatorisch belastbaren Governance. Aus einem technisch nachvollziehbaren Änderungsprotokoll wird beispielsweise nicht automatisch ein fachlicher Freigabenachweis.

³ Andrej Karpathy, „LLM Wiki“, GitHub Gist vom 4. April 2026, <https://gist.github.com/karpathy/442a6bf555914893e9891c11519de94f>.

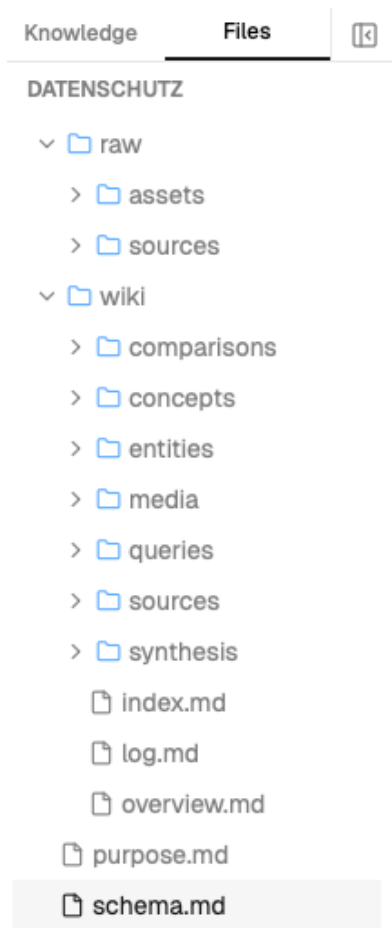


Abbildung 1: Grundstruktur des LLM-Wikis mit Rohquellen, Wiki, Schema, Index und Log

4 Nicht jedes Wissen gehört in dasselbe System

Für den Einsatz in einer Datenschutzfunktion genügt es nicht, alle auffindbaren Inhalte in ein gemeinsames Wiki zu überführen. Zunächst muss unterschieden werden, um welche Art von Wissen es sich handelt, wem es zuzurechnen ist und wie es aktualisiert werden kann.

Fachwissen umfasst insbesondere Rechtsnormen, Rechtsprechung, Positionen von Aufsichtsbehörden, Literatur und allgemein einsetzbare Prüfschemata. Dieses Wissen kann in einem redaktionell betreuten LLM-Wiki abgebildet werden. Dabei muss sichtbar bleiben, ob eine Seite eine Primärquelle wiedergibt, eine Zusammenfassung enthält oder eine eigene fachliche Bewertung darstellt.

Organisationswissen betrifft Prozesse, Systeme, Zuständigkeiten, Rollen, Richtlinien und getroffene Entscheidungen. Eigentümer dieses Wissens ist regelmäßig die Organisation, nicht die einzelne Person, die den Inhalt dokumentiert hat. Teile davon eignen sich für ein Wiki; strukturierte Informationen können besser in Datenbanken und umfangreiche Originaldokumente besser in einem Dokumentenmanagement- oder RAG-System aufgehoben sein.

Bisherige Arbeitsergebnisse der Datenschutzfunktion umfassen Beratungen, Datenschutz-Folgenabschätzungen, Vertragsprüfungen und Stellungnahmen. Sie sind besonders wertvoll, weil sie die tatsächliche Bewertungspraxis abbilden. Zugleich sind sie häufig fallbezogen, vertraulich und mit personenbezogenen Informationen verbunden. Für die Wissensbasis sollte deshalb nicht ohne Weiteres das vollständige Arbeitsergebnis übernommen werden. Häufig ist eine abstrahierte und freigegebene Bewertungslinie geeigneter als die vollständige Akte.

Arbeitsergebnisse anderer Organisationseinheiten können für den DSB relevant sein, stehen aber nicht automatisch in seiner redaktionellen Verantwortung. Hier müssen Zuständigkeiten, Herkunft und Freigabestatus erkennbar bleiben.

Persönliches Wissen betrifft Sprache, Tonalität, Arbeitspräferenzen, individuelle Ziele und private Notizen. Dieses Wissen passt eher in ein persönliches Second Brain oder in eine kontrollierte Memory-Funktion des Harness. Es darf nicht unbemerkt zum vermeintlichen Organisationswissen werden.

Diese Trennung zeigt einen wesentlichen Unterschied zwischen Second Brain und LLM-Wiki. Ein Second Brain darf subjektiv, vorläufig und auf die Arbeitsweise einer Person zugeschnitten sein. Ein organisationsweit eingesetztes LLM-Wiki benötigt dagegen Redaktion, Herkunftsnachweise, Zuständigkeiten und Freigabestatus. Je stärker es als Grundlage für Beratungen dient, desto weniger darf es wie ein privates Notizbuch behandelt werden.

5 LLM-Wiki und RAG ergänzen sich

LLM-Wiki und RAG werden gelegentlich als konkurrierende Ansätze dargestellt. Für die Praxis ist diese Gegenüberstellung wenig hilfreich. Sie lösen unterschiedliche Aufgaben.

RAG beantwortet vor allem die Frage: **Welche Quellen benötigt das Modell für diese konkrete Anfrage?** Das Verfahren ist besonders nützlich bei großen, dynamischen oder fallbezogenen Dokumentenbeständen. Dazu gehören aktuelle Rechtsquellen, neue Orientierungshilfen, Vertragsversionen, Vorgangsakten und Dokumente, deren Zugriff von der Rolle des jeweiligen Nutzers abhängt.

Das LLM-Wiki beantwortet dagegen die Frage: **Wie wird aus Quellen dauerhaft nutzbares Fachwissen?** Seine Stärke liegt in kuratierten Begriffen, stabilen Bewertungslinien, Querverbindungen, Prüfschemata und fachlichen Synthesen. Ein Wiki-Eintrag zur Datenschutz-Folgenabschätzung kann etwa die maßgeblichen Rechtsgrundlagen, typische Auslösekriterien, wiederkehrende Sachverhaltsfragen und Verweise auf Risikokataloge zusammenführen.

Die Schwächen entsprechen den jeweiligen Stärken. Ein RAG-System kann unpassende Textausschnitte finden, den Kontext eines Dokuments verfehlen oder relevante Quellen übersehen. Ein LLM-Wiki kann veralten, eine fehlerhafte Zusammenfassung fortschreiben oder eine frühere Einzelfallbewertung unzulässig verallgemeinern.

Für die Datenschutzfunktion ergibt sich deshalb ein kombiniertes Zielbild:

- Das LLM-Wiki enthält freigegebene und wiederverwendbare Bewertungslinien, Begriffe, Prüfschemata und organisationsbezogene Zusammenhänge.
- RAG stellt aktuelle Primärquellen, große Dokumentenbestände und fallbezogene Unterlagen bereit.
- Der AI Harness steuert, welche Wissensräume und Quellen für eine Aufgabe herangezogen werden.
- Der DSB prüft das Ergebnis und entscheidet, ob neue Erkenntnisse in die Wissensbasis zurückgeführt werden.

Der Unterschied lässt sich in einem Merksatz verdichten: **Das LLM-Wiki macht Antworten anschlussfähig. RAG macht sie aktualisierbar.**

6 Praxisbeispiel: Ein Datenschutz-Wiki

Ein experimentelles Datenschutz-Wiki kann mit einer einfachen Dateistruktur beginnen. Die Rohquellen werden unverändert abgelegt oder eindeutig referenziert. Daneben entstehen Wiki-

Seiten, die das enthaltene Wissen verdichten. Eine Schema-Datei beschreibt, wie der Agent mit den Inhalten umgehen soll. Index und Log unterstützen Navigation und Nachvollziehbarkeit.

Entscheidend ist eine purpose.md, die Zweck, Leitfragen und Grenzen des Wikis festlegt. Ein Datenschutz-Wiki sollte nicht „alles über Datenschutz“ enthalten. Es kann beispielsweise auf die Beratung zu DSGVO, BDSG und einem bestimmten Landesdatenschutzgesetz, auf Auftragsverarbeitung, Datenschutz-Folgenabschätzung und KI-bezogene Verarbeitungssituationen begrenzt werden. Ebenso wichtig ist die Festlegung, was nicht in das Wiki gehört.

Project Purpose

[Links](#) [Edit](#)

Goal

Diese LLM Wiki dient als strukturierte Wissensbasis zum Datenschutzrecht, erstellt von Stephan Rehfeld (DSB der TU Braunschweig). Sie versorgt das dienstliche Profil (TU Braunschweig) und das BvD-Profil mit verlässlichem, belegbarem Wissen zu DSGVO, BDSG, NDSG, europäischer Rechtsprechung, Aufsichtsbehörden-Positionen und praktischen Datenschutzfragen.

Key Questions

Welche Rechtsgrundlagen nach DSGVO greifen für welche Verarbeitungssituation?
Welche EuGH- und BVerfG-Rechtsprechung ist für die aktuelle Praxis relevant?
Welche Positionen vertreten die Aufsichtsbehörden (EDPB, DSK, LfD Niedersachsen)?
Wie sind nationale Besonderheiten (BDSG, NDSG, TTDG/TDDG) ausgestaltet?
Welche Pflichten, Rechte und Verfahren ergeben sich aus der DSGVO für Verantwortliche und Auftragsverarbeiter?
Wie sind Betroffenenrechte (Art. 15–22 DSGVO) konkret umzusetzen?
Welche Anforderungen gelten für DSFA, VVT, AVV und andere Dokumentationspflichten?
Welche Besonderheiten gelten im Beschäftigten- und Forschungskontext (§ 12/13 NDSG)?

Scope

In scope:

DSGVO (sämtliche Regelungsbereiche: Grundsätze, Rechtsgrundlagen, Betroffenenrechte, Pflichten, DSFA, AVV, Aufsicht, Sanktionen)
BDSG und landesrechtliche Regelungen (insb. NDSG)
EuGH- und BVerfG-Rechtsprechung zum Datenschutz
EDPB-Leitlinien und DSK-Beschlüsse
Bitkom-Leitfäden und Praxis-papiere
Beschäftigtendatenschutz (§ 12 NDSG, § 26 BDSG)
Forschungskontext (§ 13 NDSG)
KI-Verordnung (AI Act) mit Schnittstellen zum Datenschutz
Telekommunikation und digitale Dienste (TDDG/TTDGS)
Auftragsverarbeitung und gemeinsame Verantwortlichkeit (Art. 26, 28 DSGVO)
Datenschutz-Folgenabschätzung (DSFA)
Betroffenenrechte
Verhaltensregeln (Art. 40 DSGVO) und Zertifizierung (Art. 42 DSGVO)

Out of scope:

Hochschul-/TU-spezifische Governance-Dokumente (dafür gibt es die TU-Governance-Wiki)
Allgemeines Beamtenrecht, öffentliches Dienstrecht (nur soweit Schnittstelle zu Datenschutz)
Urheberrecht (außer bei Foto-/Videoaufnahmen mit Personenbezug)
IT-Sicherheitstechnik (nur soweit TOMs-Bezug)

Abbildung 2: Zweck und Scope des Datenschutz-Wikis des Autors

Auch die Seitentypen sollten vorab bestimmt werden. Eine **Quellenseite** dokumentiert ein Ausgangsdokument. Eine **Entity-Seite** beschreibt beispielsweise eine Aufsichtsbehörde, einen Anbieter oder ein Informationssystem. Eine **Konzeptseite** erläutert einen Fachbegriff. Eine **Comparison-Seite** vergleicht Regelungen oder Positionen. Eine **Synthesis-Seite** führt mehrere Quellen zu einer fachlichen Einordnung zusammen. Eine **Query-Seite** kann eine offene Untersuchung dokumentieren.

Diese Typisierung verhindert zwar nicht automatisch Fehler, macht aber die Funktion einer Seite sichtbar. Gerade für juristische Arbeit ist die Trennung wichtig: Der Wortlaut einer Norm, die Zusammenfassung einer Orientierungshilfe, die Bewertung des DSB und ein ungeprüfter Arbeitsstand dürfen nicht ineinanderfallen.

Page Types

Type	Directory	Purpose
entity	wiki/entities/	Named things (people, tools, organizations, datasets)
concept	wiki/concepts/	Ideas, techniques, phenomena, frameworks
source	wiki/sources/	Papers, articles, talks, books, blog posts
query	wiki/queries/	Open questions under active investigation
comparison	wiki/comparisons/	Side-by-side analysis of related entities
synthesis	wiki/synthesis/	Cross-cutting summaries and conclusions
overview	wiki/	High-level project summary (one per project)

Abbildung 3: Seitentypen des Datenschutz-Wikis

Als konkretes Beispiel kann eine Entity-Seite zur Datenschutzkonferenz dienen. Sie beschreibt Aufgabe und Zusammensetzung, verweist auf Quellen, enthält Tags und verknüpft die DSK mit Themen wie Datenschutz-Folgenabschätzung, Standard-Datenschutzmodell oder KI. Aus einem Suchbegriff wird damit ein fachlicher Knoten in einem Wissensnetz.

datenschutzkonferenz.md

Datenschutzkonferenz

ENTITY 2026-07-20 dsk aufsicht datenschutz bundeslaender dsgvo koordinierung gremium koordination deutschland

kooperation ds-gvo konferenz bundesland

Sources (15)

- Tätigkeitsberichte/Berlin/...
- Tätigkeitsberichte/BfDI/2...
- Tätigkeitsberichte/LDA Ba...
- Tätigkeitsberichte/LDI NR...
- Tätigkeitsberichte/LDI NR...
- Tätigkeitsberichte/LFD Nie...
- Tätigkeitsberichte/LFD Nie...
- Tätigkeitsberichte/Rheinla...
- Tätigkeitsberichte/Rheinla...
- Tätigkeitsberichte/Rheinla...
- Tätigkeitsberichte/Thüring...
- Tätigkeitsberichte/Thüring...
- Tätigkeitsberichte/Thüring...
- Tätigkeitsberichte/ULD Sc...
- Tätigkeitsberichte/ULD Sc...

Related (42)

- aufsichtsbehoerde
- buessgeldzumessung-nach-dsgvo
- kohärenzverfahren
- one-stop-shop-prinzip
- bundesbeauftragter-fuer-den-datensch...
- europaeischer-datenschutz-ausschuss
- transportverschlüsselung
- bayerisches-landesamt-fuer-datensch...
- tracking-tools-und-einwilligung
- facebook-fanpages-und-gemeinsame...
- ldi-nrw
- positivdaten
- selbstbindungsmechanismus-der-dsk
- institutionalisierung-der-dsk
- marktüberwachung-von-ki-systemen
- landesbeauftragte-fuer-den-datensch...
- standard-datenschutzmodell
- corona-warn-app
- luca-app
- digitale-kontaktverfolgung
- privacy-by-design
- kuenstliche-intelligenz-und-datenschu...
- oeffentlichkeitsarbeit-einer-datenschut...
- ak-dsk-2-0
- koordinierte-datenschutz-aufsicht-uebe...
- staendige-geschaeftsstelle-der-dsk
- thueringer-landesbeauftragter-fuer-den...
- bfdi
- verhaltensbasierte-werbung
- datencockpit
- profiling
- thueringer-landesbeauftragter-fuer-de...
- bsi
- microsoft
- edpb
- ki-verordnung-und-datenschutz
- nationale-zustaendigkeiten-fuer-die-ki...
- menschenzentrierte-digitalisierung-in...
- uld-schleswig-holstein
- datenschutz-folgenabschaetzung
- standardvertragsklauseln-als-transfери...
- drittlanduebermittlung-medizinische-fo...

More updated: 2026-07-20

Datenschutzkonferenz

Die Datenschutzkonferenz (DSK) ist der Zusammenschluss beziehungsweise das koordinierende Gremium der deutschen Datenschutzaufsichtsbehörden. Sie erscheint in den Quellen als Koordinationsrahmen für gemeinsame Orientierungshilfen, Positionspapiere, Entschlüsse, Beschlüsse und abgestimmte Aufsichtspraxis. Damit dient sie als Instrument zur Harmonisierung der Aufsicht und als Plattform für gemeinsame Bewertungen zwischen Bund und Ländern.

Die Quellen beschreiben die DSK zugleich als fachlich einflussreich, aber institutionell nur begrenzt abgesichert. Ihre Arbeit übersetzt abstrakte Vorgaben des Datenschutzrechts in anwendbare Prüfpunkte und einheitliche Bewertungen. Neuere Berichte ergänzen, dass sich ihre institutionelle Weiterentwicklung zunehmend in den Mittelpunkt rückt.

Rolle und Funktion

Die DSK dient dazu, die Praxis der Aufsichtsbehörden zu koordinieren und einheitliche Bewertungen zu fördern. Ihre Kriterien und Positionen übersetzen abstrakte gesetzliche Anforderungen in anwendbare Prüfpunkte.

In den Berichten wird ihr Nutzen für gemeinsame Leitlinien und abgestimmte Aufsichtspraxis ebenso hervorgehoben wie der Bedarf an klareren

Abbildung 4: Entity-Seite zur Datenschutzkonferenz

Für die praktische Arbeit könnten unter anderem folgende Wissensbereiche aufgebaut werden:

- Rollen, Rechtsgrundlagen und Betroffenenrechte,
- Auftragsverarbeitung und typische Vertragsklauseln,
- Datenschutz-Folgenabschätzung mit wiederverwendbaren Sachverhaltsfragen,
- Aufsichtsbehördenpositionen und Rechtsprechung,
- KI-spezifische Verarbeitungssituationen,
- organisationsinterne Zuständigkeiten und freigegebene Bewertungslinien.

Der Nutzen liegt nicht darin, dass das Wiki eine abschließende rechtliche Bewertung automatisch erzeugt. Es soll die Vorarbeit verbessern: einschlägige Zusammenhänge sichtbar machen, frühere Bewertungen auffinden, offene Fragen benennen und eine strukturierte Erstfassung erstellen.

7 Der AI Harness als Arbeitsumgebung

Ein LLM kann eine Markdown-Datei lesen. Für die fortlaufende Arbeit mit einem LLM-Wiki reicht dieser Einzelzugriff jedoch nicht aus. Das System muss mehrere Dateien durchsuchen, Seiten erstellen und aktualisieren, Quellen einbinden, Änderungen protokollieren und gegebenenfalls verschiedene Modelle oder Werkzeuge verwenden können. Diese Funktionen übernimmt der AI Harness.

Der Harness kann insbesondere festlegen:

- auf welche Dateien und Wissensräume ein Modell zugreifen darf,
- welche Werkzeuge zur Verfügung stehen,
- ob nur gelesen oder auch geschrieben werden darf,
- welches Modell für eine Aufgabe eingesetzt wird,
- ob eine Antwort mit aktuellen Quellen ergänzt werden muss,
- welche Änderungen einer menschlichen Prüfung bedürfen,
- welche Informationen als temporärer Kontext oder dauerhaftes Memory behandelt werden.

In einem experimentellen Aufbau wurde hierfür Hermes Agent eingesetzt, ein quelloffener Agent, der Modelle mit Dateien und Werkzeugen verbinden kann.⁴ Ein denkbarer Arbeitsablauf beginnt mit einer Praxisfrage des DSB. Der Agent sucht passende Wiki-Seiten, erstellt eine strukturierte Erstfassung mit Sachverhaltsfragen, rechtlichen Anknüpfungspunkten und offenen Prüfpunkten. Der DSB korrigiert diese Fassung. Erst danach wird entschieden, ob eine abstrahierte Erkenntnis, ein verbessertes Prüfschema oder eine neue Verknüpfung in das Wiki zurückfließt.

Der Harness ist damit nicht nur eine technische Bedienoberfläche. Er ist die Stelle, an der organisatorische Regeln in Arbeitsabläufe übersetzt werden können. Er ersetzt diese Regeln jedoch nicht. Eine Schreibsperrung bildet beispielsweise noch keinen fachlichen Freigabeprozess ab, solange nicht bestimmt ist, wer nach welchen Kriterien freigibt.

8 Derselbe Prompt, zwei unterschiedliche Antworten

Der praktische Mehrwert eines LLM-Wikis lässt sich an einem Vergleich zeigen. Zwei Systeme erhielten dieselbe Frage: Wie lange muss ein Wissenschaftler der TU Braunschweig personenbezogene Daten aus einer empirischen Forschungsarbeit aus datenschutzrechtlichen Gründen aufbewahren, und welche Rechtsgrundlagen sind heranzuziehen?

⁴ Nous Research, „Hermes Agent“, GitHub, <https://github.com/NousResearch/hermes-agent>.

Eine Antwort wurde mit Hermes Agent und Zugriff auf das Datenschutz-Wiki erzeugt. Die andere stammte von einem allgemeinen LLM ohne Zugriff auf dieses Wiki.

Beide Antworten erkannten den Ausgangspunkt: Es gibt keine für alle Forschungsprojekte geltende datenschutzrechtliche Aufbewahrungsfrist. Maßgeblich sind insbesondere der Grundsatz der Speicherbegrenzung aus Art. 5 Abs. 1 Buchst. e DSGVO, die Anforderungen des Art. 89 DSGVO und der konkrete Forschungszweck.⁵

Die Antwort mit LLM-Wiki war deutlich organisationsnäher. Sie bezog die TU Braunschweig, das niedersächsische Landesrecht und den Forschungskontext ein. Sie nannte § 13 NDSG, unterschied mehrere Projektphasen und schlug konkrete Arbeitsschritte vor, etwa einen Forschungsdatenmanagementplan, die Trennung von Identifikatoren und Forschungsdaten sowie eine differenzierte Löschung.⁶ Die Antwort ohne Wiki blieb allgemeiner. Sie verwies auf die DSGVO, die gute wissenschaftliche Praxis sowie interne Stellen, lieferte aber weniger organisationsspezifische Substanz.

Damit zeigt sich ein realer Vorteil: Das LLM-Wiki kann aus einer allgemeinen Rechtsfrage eine organisationsnahe Beratungsskizze machen. Es kann lokale Normen, interne Begriffe, bekannte Prozesse und frühere Bewertungslinien einbeziehen. Das Ergebnis ist leichter in die weitere Arbeit des DSB zu überführen.

Gerade diese Stärke erzeugt jedoch ein zusätzliches Risiko. Die konkretere Antwort wirkt belastbarer, obwohl einzelne Aussagen erst geprüft werden müssen. So enthält § 13 Abs. 1 NDSG nicht lediglich ein abstraktes Erforderlichkeitskriterium, sondern eine Interessenabwägung mit Aufzeichnungs- und Unterrichtungspflichten; Abs. 2 verlangt die Anonymisierung, sobald dies nach dem Forschungszweck möglich ist, und bis dahin die getrennte Speicherung der Identifikationsmerkmale.⁷ Auch eine in der Antwort genannte Frist von „oft 2–3 Jahren“ für bestimmte personenbezogene Unterlagen wurde nicht mit einer Quelle belegt. Die zehnjährige Sicherung von Forschungsdaten folgt wiederum aus der guten wissenschaftlichen Praxis und ist nicht mit einer pauschalen datenschutzrechtlichen Erlaubnis zur zehnjährigen Speicherung identifizierbarer Daten gleichzusetzen.⁸

Der Vergleich belegt deshalb nicht, dass die Antwort mit LLM-Wiki in jeder Hinsicht „richtiger“ war. Er belegt, dass sie **anschlussfähiger und konkreter** war. Genau deshalb war sie auch **prüfbedürftiger**. Ein allgemeines Modell kann wichtige lokale Zusammenhänge übersehen. Ein LLM-Wiki kann dagegen unzutreffende lokale Zusammenhänge besonders überzeugend präsentieren.

Ohne RAG oder eine andere aktuelle Quellenanbindung erkennt das System zudem nicht notwendig, ob eine Norm geändert, eine Orientierungshilfe veröffentlicht oder eine interne Richtlinie ersetzt wurde. Was im Wiki fehlt, kann für das Modell unsichtbar bleiben. Was im Wiki falsch verdichtet wurde, kann in späteren Antworten weiterleben.

⁵ Art. 5 Abs. 1 Buchst. e und Art. 89 DSGVO, <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32016R0679>.

⁶ § 13 NDSG in der geltenden Fassung sowie die Erläuterungen des Landesbeauftragten für den Datenschutz Niedersachsen, <https://voris.wolterskluwer-online.de/browse/document/29810db4-2ea9-3bfb-b3c2-47c2b52f1665> und <https://www.lfd.niedersachsen.de/forschung/datenschutz-und-forschung-56093.html>.

⁷ § 13 NDSG in der geltenden Fassung sowie die Erläuterungen des Landesbeauftragten für den Datenschutz Niedersachsen, <https://voris.wolterskluwer-online.de/browse/document/29810db4-2ea9-3bfb-b3c2-47c2b52f1665> und <https://www.lfd.niedersachsen.de/forschung/datenschutz-und-forschung-56093.html>.

⁸ Deutsche Forschungsgemeinschaft, „Leitlinien zum Umgang mit Forschungsdaten“, insbesondere zur mindestens zehnjährigen Archivierung nach den Regeln guter wissenschaftlicher Praxis, <https://www.dfg.de/resource/blob/172112/4ea861510ea369157afb499e96fb359a/leitlinien-forschungsdaten-data.pdf>.

9 Governance entscheidet über den professionellen Nutzen

Ein persönliches LLM-Wiki lässt sich mit wenigen Dateien aufbauen. Für eine Datenschutzfunktion oder eine Organisation stellen sich deutlich anspruchsvollere Fragen.

9.1 Zweck und Scope

Vor der ersten Quelle muss feststehen, welche Aufgaben das Wiki unterstützen soll. Ein Wiki für allgemeines Datenschutzwissen benötigt andere Inhalte als ein Wiki für organisationsinterne Beratung oder einen bestimmten Mandanten. Ein zu weiter Scope führt dazu, dass unterschiedliche Wissensarten, Verantwortlichkeiten und Schutzbedarfe miteinander vermischt werden.

9.2 Herkunft und Status

Jede fachlich relevante Aussage sollte auf ihre Herkunft zurückgeführt werden können. Ebenso muss erkennbar sein, ob es sich um eine Primärquelle, eine Zusammenfassung, eine eigene Bewertung, einen Entwurf oder eine freigegebene Bewertungslinie handelt. Ohne diese Kennzeichnung entsteht ein einheitlich formulierter Wissensbestand, der Unterschiede in der Verbindlichkeit verdeckt.

9.3 Redaktion und Freigabe

Es muss festgelegt werden, wer neue Inhalte einstellen, ändern und freigeben darf. Eine automatische Wiki-Aktualisierung sollte zunächst als Änderungsvorschlag behandelt werden. Für zentrale Bewertungslinien kann ein Vier-Augen-Prinzip sinnvoll sein. Freigabe bedeutet dabei mehr als die Bestätigung, dass ein Text sprachlich plausibel ist. Geprüft werden müssen Quellen, Reichweite, Aktualität und die zulässige Übertragbarkeit auf andere Fälle.

9.4 Aktualisierung

Rechtsnormen, Aufsichtsbehördenpositionen, Anbieterbedingungen und interne Richtlinien ändern sich. Wiki-Seiten benötigen deshalb Verantwortliche, Aktualisierungsdaten und Wiedervorlagen. Linting kann auf möglicherweise veraltete Seiten oder Widersprüche hinweisen, aber nicht abschließend entscheiden, welche Rechtsauffassung gilt.

Review **383**
Refresh Clear resolved

☐ Select pending
0 selected
Mark selected resolved
Dismiss selected

☐ **§ 38 BDSG versus „BDSG-neu“**
×

Das Wiki verwendet sowohl '§ 38 BDSG' als auch die ältere Bezeichnung 'BDSG-neu'. Das sollte geprüft und vereinheitlicht werden, damit die Seiten nicht historisch und aktuell gleichzeitig unterschiedliche Normbezeichnungen suggerieren.

Pages: [wiki/concepts/benennungspflicht-nach-bdsg.md](#), [wiki/concepts/benennungspflicht-eines-datenschutzbeauftragten.md](#), [wiki/sources/benennung-eines-datenschutzbeauftragten.md](#)

Create Page
Skip

☐ **Zeitstempel der generierten Wiki-Dateien**
×

Die erzeugten Dateien sind mit 'created: 2026-07-20' und 'updated: 2026-07-20' versehen, obwohl der aktuelle Bearbeitungszeitpunkt im Workspace auf den 2026-07-19 fällt. Das sollte geprüft werden, damit die Wiki-Metadaten konsistent bleiben.

Pages: [wiki/sources/Datenschutz-in-Wissenschaft.md](#), [wiki/concepts/wissenschaftliche-forschung-im-datenschutzrecht.md](#), [wiki/concepts/archivierung-im-oeffentlichen-interesse.md](#)

Create Page
Skip

☐ **Aktuelle DSK-Kriterien und Listen zur DSFA-Pflicht verifizieren**
×

Die Quelle stützt sich auf die abgestimmte DSK-Liste und eine mögliche Negativliste nach Art. 35 Abs. 4 und 5 DSGVO. Diese Konkretisierung ist praxisrelevant, aber revisionsanfällig; hier sollte die aktuell gültige Fassung der DSK-Orientierung und die zuständige Aufsichtsbehördenpraxis gezielt nachrecherchiert werden.

Pages: [wiki/entities/datenschutzkonferenz.md](#), [wiki/concepts/datenschutzfolgenabschätzung.md](#)

Deep Research
Create Page
Skip

☐ **Cloud-Hosting-Hinweis für medizinische Daten in bayerischen Krankenhäusern**
×

Der Hinweis, dass Cloud-Hosting medizinischer Daten in bayerischen Krankenhäusern für Labore und andere Einrichtungen „unzulässig sein kann“, ist stark kontextabhängig und im Wiki leicht zu verallgemeinern. Das sollte fachlich gegengeprüft werden, bevor daraus ein allgemeines Cloud-Verbot oder eine breite Konzeptaussage abgeleitet wird.

Pages: [wiki/sources/10-ida-bayern--23-bayldachecklistemedizin--tox0lzm.md](#), [wiki/concepts/cloud-dienste-im-datenschutz.md](#)

Create Page
Skip

☐ **Aktueller Rechtsstatus des EU-U.S. Data Privacy Framework**
×

Die Quelle ist zeitlich sensibel und verweist selbst auf eine mögliche spätere EuGH-Prüfung. Es sollte verifiziert werden, ob der EU-U.S. DPf zum heutigen Rechtsstand weiterhin gilt, ob es seit dem Angemessenheitsbeschluss vom 10. Juli 2023 gerichtliche Entscheidungen, Aussetzungen oder Anpassungen gab und wie Aufsichtsbehörden das aktuell einordnen.

Pages: [wiki/concepts/eu-us-data-privacy-framework.md](#), [wiki/concepts/angemessenheitsbeschluss.md](#)

Deep Research
Create Page
Skip

☐ **Abgrenzung der DPF-Rechtsschutzseiten**
×

Die neu angelegten Seiten 'rechtsschutz-im-eu-us-dpf', 'beschwerdeverfahren-nach-eu-us-dpf' und 'beschwerden-zur-nationalen-sicherheit-im-eu-us-dpf' überlappen inhaltlich stark. Es sollte geprüft werden, ob daraus eine einzige Hauptseite mit Unterabschnitten werden sollte oder ob die Trennung nach Rechtsschutzarten fachlich dauerhaft sinnvoll ist.

Pages: [wiki/concepts/rechtsschutz-im-eu-us-dpf.md](#), [wiki/concepts/beschwerdeverfahren-nach-eu-us-dpf.md](#), [wiki/concepts/beschwerden-zur-nationalen-sicherheit-im-eu-us-dpf.md](#)

Create Page
Skip

Abbildung 5: Vom System identifizierte Review-Punkte

9.5 Korrektur und Löschung

Eine fehlerhafte Aussage kann an mehreren Stellen fortwirken: auf einer Quellenseite, in einer Synthese, im Index, in einer späteren Beratung, in einem Suchindex oder in einer Memory-Funktion. Die Korrektur einer einzelnen Markdown-Datei genügt dann nicht. Erforderlich ist ein Verfahren, das abgeleitete Inhalte identifiziert und gegebenenfalls neu erzeugt. Entsprechendes gilt für Löschanforderungen.

9.6 Berechtigungen und Wissensräume

Öffentliche Quellen, interne Richtlinien, vertrauliche Beratungen, DSFA-Unterlagen und persönliche Notizen dürfen nicht automatisch in denselben Kontext gelangen. Häufig wird nicht ein einziges Wiki, sondern eine Trennung nach Wissensräumen erforderlich sein. Die Berechtigung muss sich sowohl auf das Lesen als auch auf das Schreiben, Rückführen und Zusammenführen von Wissen beziehen.

9.7 Datenschutzrechtliche Einordnung des Betriebs

Enthält das Wiki personenbezogene Daten, ist sein Betrieb selbst eine Verarbeitung. Zweck, Rechtsgrundlage, Datenminimierung, Speicherbegrenzung, Betroffenenrechte, Verantwortlichkeiten und gegebenenfalls eine Datenschutz-Folgenabschätzung sind daher gesondert zu beurteilen. Die Tatsache, dass eine Information für spätere Beratungen nützlich sein könnte, bildet noch keine eigenständige Rechtsgrundlage für ihre dauerhafte Aufnahme.

Ein allgemein etablierter Enterprise-Standard, der LLM-Wiki, RAG, differenzierte Berechtigungen, Freigabe, Versionierung, Löschung und fachliche Review in einem Produkt vollständig zusammenführt, ist derzeit nicht erkennbar. Verfügbare Werkzeuge decken Teilfunktionen ab. Für den professionellen Einsatz muss deshalb geprüft werden, welche organisatorischen Anforderungen technisch unterstützt werden und welche durch zusätzliche Prozesse abgesichert werden müssen.

10 Taxonomien, Ontologien und Modellwahl

Mit wachsendem Umfang reicht eine Sammlung gut geschriebener Seiten nicht aus. Das Wiki benötigt eine gemeinsame Sprache.

Eine **Taxonomie** ordnet Inhalte nach vorgegebenen Kategorien, beispielsweise Rechtsgrundlage, Rolle, Verarbeitungssituation, Risiko, Maßnahme, Dokumenttyp oder Freigabestatus. Sie verbessert Navigation und Suche und kann Zuständigkeiten sichtbar machen.

Eine **Ontologie** beschreibt darüber hinaus Beziehungen zwischen Begriffen. Eine Verarbeitungstätigkeit hat etwa einen Verantwortlichen, betrifft bestimmte Personengruppen, verfolgt Zwecke, verwendet Datenkategorien, ist mit Risiken verbunden und wird durch Maßnahmen abgesichert. Solche Beziehungen können in Links, Metadaten oder einem Wissensgraphen abgebildet werden.



Abbildung 6: Wissensgraph des Datenschutz-Wikis des Autors

Für die Praxis gilt: Die Struktur muss dem Arbeitszweck dienen. Eine zu feine Ontologie erzeugt erheblichen Pflegeaufwand und kann dem Modell eine nicht vorhandene fachliche Eindeutigkeit vorspiegeln. Zweckmäßiger ist ein schrittweiser Ausbau anhand tatsächlich wiederkehrender Beratungsfragen.

Auch das eingesetzte LLM beeinflusst das Ergebnis. Allgemeine Modelle sind häufig stark bei Sprache, Zusammenfassung und Strukturierung. Juristisch spezialisierte Modelle oder Arbeitsumgebungen können Vorteile bei Fachsprache, Quellenzugang und juristischen Aufgaben bieten. Beck-Noxtua ist ein Beispiel für eine juristische KI-Arbeitsumgebung, die Inhalte von beck-online mit einem auf den Rechtsbereich ausgerichteten KI-System verbindet.⁹

Die Modellwahl löst jedoch nicht das Wissensproblem. Ein spezialisiertes Modell kennt nicht automatisch die Organisation. Umgekehrt macht ein organisationsspezifisches Wiki aus einem ungeeigneten Modell kein verlässliches Rechtssystem. Fachmodell, aktuelle Quellen und organisationsbezogenes Wissen sind unterschiedliche Komponenten.

11 Praxistipp: Das Konzept mit überschaubarem Aufwand erproben

Für einen ersten Versuch ist keine vollständige Plattform erforderlich. Karpathys LLM-Wiki-Gist kann einem dateibasierten AI Harness beziehungsweise LLM-Agenten als Ausgangsanweisung übergeben werden. Der Agent kann daraus gemeinsam mit dem Nutzer eine passende Verzeichnisstruktur, ein Schema, Seitentypen und Arbeitsabläufe entwickeln. Geeignet sind Harnesses, die kontrolliert auf einen lokalen Projektordner zugreifen und Markdown-Dateien lesen sowie ändern können.¹⁰

Eine Alternative ist das quelloffene Projekt [nashsu/llm_wiki](https://github.com/nashsu/llm_wiki). Es setzt Karpathys abstraktes Muster als Desktop-Anwendung um. Nach Angaben des Projekts unterstützt es unter anderem den Import verschiedener Dokumente, strukturierte Wiki-Seiten, einen Wissensgraphen, Review-Funktionen und optionale Vektorsuche.¹¹ Damit lässt sich das Konzept ohne eigenen Aufbau der gesamten Bedienoberfläche erproben.

Praxistipp

1. Einen eng begrenzten Zweck wählen, beispielsweise öffentliche Stellungnahmen zur Datenschutz-Folgenabschätzung.
2. Zunächst ausschließlich öffentliche oder künstlich erzeugte Testinhalte verwenden.
3. Quellen, Zusammenfassungen, Bewertungen und Entwürfe als getrennte Seitentypen anlegen.
4. Schreibvorgänge des Agenten grundsätzlich als Vorschläge behandeln.
5. Nach wenigen Quellen prüfen, ob Index, Links und Seitentypen die tatsächlichen Arbeitsfragen unterstützen.
6. Erst danach entscheiden, ob RAG, weitere Wissensräume oder komplexere Metadaten benötigt werden.

Die Verfügbarkeit eines Open-Source-Projekts oder eines AI Harness ist keine Aussage über die Eignung für einen produktiven Betrieb mit vertraulichen oder personenbezogenen Informationen. Lizenz, Datenflüsse, Modellanbieter, Protokollierung, Löscharbeit, Berechtigungen und organisatorische Einbettung müssen eigenständig geprüft werden. Fragen der technischen Informationssicherheit bleiben auch an dieser Stelle außerhalb des Beitrags.

⁹ C.H.BECK, „Launch von Beck-Noxtua“, 2025, <https://presse.beck.de/pressemitteilungen-archiv/2025/launch-von-beck-noxtua/>.

¹⁰ Andrej Karpathy, „LLM Wiki“, GitHub Gist vom 4. April 2026, <https://gist.github.com/karpathy/442a6bf555914893e9891c11519de94f>.

¹¹ nashsu, „LLM Wiki“, GitHub, https://github.com/nashsu/llm_wiki.

12 Fazit

Ein LLM-Wiki ist für Datenschutzbeauftragte keine weitere Ablage und kein automatischer Rechtsberater. Es ist ein Muster für eine Wissensinfrastruktur, in der Quellen, Begriffe, Bewertungslinien und Arbeitsergebnisse dauerhaft miteinander verbunden werden. Sein besonderer Nutzen liegt in der Wiederverwendung: Erkenntnisse aus einer Beratung müssen nicht im Chat oder in einer einzelnen Akte verschwinden, sondern können nach Prüfung in abstrahierter Form zum gemeinsamen Wissensbestand beitragen.

RAG bleibt erforderlich, wenn aktuelle Primärquellen, große Dokumentenmengen oder fallbezogene Unterlagen herangezogen werden sollen. Der AI Harness verbindet Modell, Wiki, RAG, Werkzeuge und Arbeitsabläufe. Ein Second Brain kann daneben das persönliche Wissen und die individuelle Arbeitsweise unterstützen, darf aber nicht ungeprüft mit dem Wissensbestand der Organisation verschmelzen.

Die größten Herausforderungen liegen derzeit nicht in der Erstellung von Markdown-Seiten. Sie liegen in Freigabe, Aktualisierung, Korrektur, Löschung, Berechtigungen, Vertraulichkeitsklassen und fachlicher Verantwortlichkeit. Gerade Datenschutzbeauftragte können zu dieser Entwicklung deshalb mehr beitragen als die Bewertung eines fertigen Werkzeugs. Sie können mitgestalten, nach welchen Regeln Wissen in KI-gestützten Arbeitsumgebungen entsteht und verwendet wird.

Die Schlussfolgerung lautet: **Das LLM-Wiki macht Wissen anschlussfähig. RAG hält den Zugang zu aktuellen Quellen offen. Der AI Harness bringt beides zusammen. Die fachliche Verantwortung bleibt beim Menschen.**

Danksagung

Ich danke Dr. Christian Böttger, CISO der TU Braunschweig, für die Stunden der Diskussion, des Ausprobierens und der vielen Ideen.

Über den Autor

Dipl.-Ök. Stephan Rehfeld ist Datenschutzbeauftragter der TU Braunschweig, stellvertretender Sprecher der Kommission IT-Recht des ZKI e.V. und Vorstand des BvD e.V.

Lizenz: Creative Commons Attribution Non Commercial No Derivatives 4.0 International