Innovation und Verantwortung
KI-Compliance in der Deutschen Nationalbibliothek

1. Die Ausgangslage

Die steigenden Anwendungsmöglichkeiten Künstlicher Intelligenz (KI) haben innerhalb weniger Jahre den Arbeitsalltag vieler Bibliotheken und Informationseinrichtungen verändert. Während zunächst vor allem generative KI-Anwendungen wie ChatGPT, Midjourney oder DeepL die öffentliche Wahrnehmung prägten, zeigt sich zunehmend, dass die Auswirkungen weit über die Nutzung einzelner Werkzeuge generativer KI hinausreichen. Bibliotheken stehen heute vor der Aufgabe, KI-Technologien nicht nur punktuell einzusetzen, sondern ihren Umgang mit ihnen organisatorisch, rechtlich und strategisch zu gestalten.

Dies gilt in besonderem Maße für die Deutsche Nationalbibliothek (DNB). Als zentrale Archivbibliothek Deutschlands erfüllt sie gemäß dem Gesetz über die Deutsche Nationalbibliothek (DNBG) einen gesetzlichen Auftrag zur Sammlung, Erschließung, dauerhaften Bewahrung und Bereitstellung des veröffentlichten kulturellen Erbes (§ 2 Nr. 1 DNBG). Die Möglichkeiten künstlicher Intelligenz eröffnen hierbei erhebliche Chancen – etwa bei der automatisierten Erschließung, der Verbesserung von Such- und Recherchefunktionen oder der Unterstützung administrativer Prozesse. Gleichzeitig wirft ihr Einsatz eine Vielzahl rechtlicher, technischer und ethischer Fragen auf.[1]

2. Die Rahmenbedingungen

2.1 Rechtlicher Rahmen

Die DNB ist eine rechtsfähige bundesunmittelbare Anstalt öffentlichen Rechts (§ 1 Abs. 2 DNBG). Sie ist damit nach den Regelungen des Grundgesetzes (GG) einerseits als Teil der mittelbaren Bundesverwaltung an Recht und Gesetz gebunden (Art. 1 Abs. 3, Art. 20 Abs. 3 GG). Andererseits hat sie als eigenständige Rechtspersönlichkeit die Möglichkeit, ihr praktisches Vorgehen innerhalb dieses rechtlichen Rahmens selbstständig und weitgehend ohne äußere Einflussmöglichkeiten zu bestimmen. Dies bedeutet eine weitgehende Gestaltungsfreiheit auch bei der Frage, wie der Einsatz von KI gestaltet, ermöglicht und begrenzt werden kann und soll. Diesen Spielraum hat die DNB – wie im Folgenden zu sehen sein wird – genutzt.

1 Dieser Beitrag bezieht sich auf den Vortrag der Autoren am 21.05.2026 auf der 114. BiblioCon in Berlin; vgl. die Folien zum Vortrag unter https://nbn-resolving.org/urn:nbn:de:0290-opus4-200842.

Die Rahmenbedingungen selbst werden im Wesentlichen durch europäisches Recht oder Rechtsakte mit starkem europarechtlichem Einfluss bestimmt. Unmittelbar mit dem Thema KI verbunden ist die europäische KI-Verordnung (KI-VO; auch als AI Act bekannt).[2] Hier werden risikobasiert insbesondere die Pflichten für Anbietende und Betreibende von KI-Anwendungen geregelt. Die Regelungen der KI-VO sind jedoch nicht die einzigen, die im Umgang mit KI beachtet werden müssen. Die europäische Datenschutz-Grundverordnung (DSGVO) gilt parallel für den Umgang mit personenbezogenen Daten auch im Kontext von KI. Der dritte zu beachtende Rechtsbereich ist das Urheberrecht, das wiederum stark von einer europarechtlichen Harmonisierung geprägt ist. Ergänzend sind auch die Vorgaben zur IT-Sicherheit zu beachten, die einerseits technisch-organisatorische Maßnahmen zum Datenschutz sind, andererseits aber auch darüber hinaus greifen.

2.2 Institutioneller Rahmen

Nachdem seit Ende 2022 zunehmend generative KI-Anwendungen für den allgemeinen Markt verfügbar waren (beginnend mit Open AIs ChatGPT), waren die konkreten rechtlichen Bedingungen zunächst noch weitgehend unklar. Hilfestellungen etwa durch Handreichungen des Bundesbeauftragten für den Datenschutz oder ähnliche Leitlinien gab es für den KI-Bereich noch nicht.[3] Gleichwohl fanden entsprechende KI-Lösungen wie in der gesamten Gesellschaft auch in der DNB bald Anwendung und ermöglichten bzw. erleichterten dienstliche Abläufe.

Vor diesem Hintergrund fand sich eine Gruppe von Kolleg*innen zusammen, um neben den bereits vorhandenen Stellen zur strategischen Steuerung (Generaldirektion, CIO) und zur operativen Betreuung von KI-Anwendungen (Zentralbereich IT) auch die rechtlichen und die IT-Sicherheit betreffenden Fragen zu besprechen und Lösungen für den dienstlichen Alltag zu finden. Diese Gruppe bestand aus zwei Vertreterinnen des Justiziariats, dem internen Datenschutz-Team (Datenschutzbeauftragter und Stellvertretung) sowie dem internen Informationssicherheitsbeauftragten. Kurze Zeit später wurde der Gruppe seitens der Generaldirektion der Auftrag erteilt, interne Leitlinien für den Umgang mit KI zu erstellen. Gleichzeitig wurde die Gruppe unter dem Namen „KI-Compliance-Office“ als Expertengremium in der genannten Zusammensetzung verstetigt.

2 VERORDNUNG (EU) 2024/1689 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=de, Stand: 21.08.2026.

3 Mittlerweile finden sich entsprechende Dokumente etwa für den Datenschutz, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: KI in Behörden – Datenschutz von Anfang an mitdenken: Handreichung der BfDI für die Bundesverwaltung, 22.12.2025.: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2025/Handreichung-KI.pdf?__blob=publicationFile&v=3, Stand: 21.08.2026; vgl. auch Bundesministerium des Innern, Leitlinien für den Einsatz Künstlicher Intelligenz in der Bundesverwaltung, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/moderne-verwaltung/ki/BMI25020-leitlinien-ki-bundesverwaltung.pdf?__blob=publicationFile&v=4, Stand: 21.08.2026.

3. Leitlinien – Policys

3.1 KI-Policy für Mitarbeitende als Nutzende

Wo innovative technische Lösungen Möglichkeiten eröffnen, die bisher kaum denkbar waren, ist ihr verantwortlicher Einsatz besonders wichtig. Verlässliche Rahmenbedingungen tragen dazu bei, KI-Anwendungen sicher in die Prozesse der DNB zu integrieren. Dabei sollen Rechtssicherheit und technologischer Fortschritt sich nicht konkurrierend gegenüberstehen. Ziel ist es, dass Mitarbeitende innerhalb eines verlässlichen Rahmens auch weiterhin mit KI experimentieren und Innovationen einbringen können. Auf dieser Basis wurden und werden auch die internen Leitlinien durch das KI-Compliance-Office erstellt.

Zunächst stand ausschließlich der Umgang von Beschäftigten mit externen, kommerziellen KI-Lösungen im Fokus der Betrachtungen. Die eingenommene Perspektive war also diejenige der Mitarbeitenden als Endnutzer*innen, unabhängig davon, ob die DNB selbst als Anbieterin oder Betreiberin der KI anzusehen ist. Die erste, bereits 2023 in Kraft getretene KI-Policy der DNB bestimmte bereits elementare Grundsätze, die bis heute an Wichtigkeit nichts eingebüßt haben. Die geltende, im Sommer 2025 revidierte und durch die Generaldirektion veröffentlichte Fassung geht in ihren Inhalten über das gesetzlich Zwingende sogar etwas hinaus, schafft dafür aber klare und in der Praxis eindeutig handhabbare Regelungen.

Im Mittelpunkt stehen dabei ein verantwortungsvoller und sicherer Einsatz in einem verlässlichen und klaren Rahmen, die Wahrung datenschutzrechtlicher und urheberrechtlicher Vorgaben sowie die fachliche Kontrolle der mit KI erzeugten Ergebnisse.[4]

Gemäß der Policy darf generative KI grundsätzlich nur unter Verwendung dienstlicher Zugänge und nur dann eingesetzt werden, wenn die betreffende Anwendung nicht von der DNB für die Nutzung gesperrt wurde. Soweit technisch möglich, sollen zudem Einstellungen gewählt werden, die eine Verwendung der eingegebenen Inhalte zu Trainingszwecken ausschließen. Besondere Bedeutung kommt der menschlichen Prüfung und Verantwortung zu. Da generative KI-Inhalte auf Grundlage statistischer Wahrscheinlichkeiten erzeugt und deren Richtigkeit nicht gewährleistet ist, dürfen KI-generierte Ergebnisse nicht ungeprüft in dienstliche Arbeitsprozesse übernommen werden. Die Verantwortung für Richtigkeit, Vollständigkeit und Rechtmäßigkeit verbleibt bei den jeweiligen Beschäftigten. KI-gestützte Inhalte sind nach Maßgabe der Richtlinie außerdem als solche kenntlich zu machen; für Veröffentlichungen und die Öffentlichkeitsarbeit gelten ergänzende Kommunikationshinweise.

Einen weiteren Schwerpunkt bildet der Schutz personenbezogener und vertraulicher Informationen.[5] Personenbezogene Daten dürfen nach der Policy grundsätzlich nicht in generative KI-Anwendungen im Einflussbereich Dritter eingegeben werden. Sollen entsprechende Inhalte verarbeitet werden, müs-

4 Herrmann, Simon: Innovation & Verantwortung: KI in der DNB, Blog der DNB, 07.08.2025, https://blog.dnb.de/innovation-verantwortung-ki-in-der-dnb/, Stand: 21.08.2026.

5 Hierzu etwa EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, 02.12.2024, https://www.edpb.europa.eu/system/files/documents/2025-05/edpb_opinion_202428_ai-models_de.pdf, Stand: 21.08.2026.

sen sie zuvor innerhalb der geschützten IT-Infrastruktur der DNB so anonymisiert werden, dass ein Personenbezug nicht mehr hergestellt werden kann. Dies ist in einer Vielzahl von Fällen vergleichsweise einfach möglich und erschwert den Einsatz von KI nicht wesentlich: Statt beispielsweise eine bestimmte Person zu adressieren, etwa in einem Mail-Entwurf, kann ein Platzhalter verwendet werden. Auch sonstige vertrauliche dienstliche Informationen, etwa interne Korrespondenz, Sitzungsprotokolle, bestimmte Inhalte aus E-Akten oder internen Informationssystemen sowie nicht für die Öffentlichkeit bestimmte Arbeitsstände, sind von der Eingabe ausgeschlossen. Enthalten KI-generierte Ergebnisse ihrerseits personenbezogene Angaben, sind diese besonders sorgfältig auf ihre Richtigkeit und die Zulässigkeit ihrer weiteren Verwendung zu prüfen.

Auch urheberrechtliche Risiken werden ausdrücklich adressiert. Der Spielraum für Bibliotheken ist hier noch nicht endgültig geklärt. Vielmehr liegt eine stetig wachsende Zahl von Entscheidungen der Instanzgerichte vor. Diese nehmen je nach zugrunde liegendem Sachverhalt unterschiedliche Aspekte der urheberrechtlichen Zulässigkeit in den Blick: Etwa die Erstellung eines Datensatzes von urheberrechtlich geschützten Daten zu Trainingszwecken[6], die Memorisierung von Werken im System und eine zufällige oder bewusste Wiedergabe[7] oder die Schutzfähigkeit generierten Inhalts.[8] Daher geht die Policy auch hier den sichersten Weg: Urheberrechtlich geschützte Werke aus den Beständen der DNB sollen nicht als Eingabedaten für generative KI-Anwendungen verwendet werden; gemeinfreie Inhalte können dagegen grundsätzlich genutzt werden. Bei der weiteren Verwendung KI-generierter Inhalte ist insbesondere zu berücksichtigen, dass diese Bestandteile geschützter Werke Dritter reproduzieren können. Vor einer Veröffentlichung ist deshalb sicherzustellen, dass keine Rechte Dritter verletzt werden.

Flankiert werden diese Vorgaben durch Schulungs- und Sensibilisierungsmaßnahmen. Die Beschäftigten sollen sowohl mit den rechtlichen Rahmenbedingungen als auch mit den technischen Grenzen und praktischen Risiken generativer KI vertraut gemacht werden. Dies setzt eine Vorgabe des Art. 4 KI-VO um, der Institutionen die Pflicht auferlegt, ihren Mitarbeitenden KI-Kompetenz zu vermitteln. Die entsprechenden Fortbildungen werden teils von Mitgliedern des KI-Compliance-Office, teils durch externe Fortbildungsanbieter abgedeckt.

6 Hanseatisches Oberlandesgericht Hamburg, Urteil vom 10.12.2025 – Az. 5 U 104/24 („LAION"), https://www.landesrecht-hamburg.de/bsha/document/NJRE001628040, Stand: 21.08.2026; zuvor Landgericht Hamburg, Urteil vom 27.09.2024 – Az. 310 O 227/23, https://www.landesrecht-hamburg.de/bsha/document/NJRE001588058, Stand: 21.08.2026; das Oberlandesgericht hielt grundsätzlich auch für diese Vorbereitungshandlungen die Schranken (gesetzlichen Erlaubnisse) für das Text-and-Data-Mining (§ 44b UrhG und § 60d UrhG) für anwendbar; das Urteil ist allerdings zum Zeitpunkt der Veröffentlichung dieses Beitrags noch nicht rechtskräftig.

7 Landgericht München I, Urteil vom 11.11.2025 – 42 O 14139/24 („GEMA ./. OpenAI"), https://www.gesetze-bayern.de/Content/Document/Y-300-Z-GRURRS-B-2025-N-30204, Stand: 21.08.2026; ähnlich auch Landgericht München I, Urteil vom 31.07.2026 – 42 O 763/25 („GEMA ./. Suno"), https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2026-N-17961?hl=true, Stand: 21.08.2026.

8 Amtsgericht München, Urteil vom 13.02.2026 – 142 C 9786/25, https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2026-N-1513, Stand: 21.08.2026, das die Schutzfähigkeit nur dann annimmt, wenn menschliche, in das Prompting eingeflossene Elemente derart dominieren, dass der Gegenstand insgesamt einer (normalen) menschlichen Schöpfung gleichkommt. Das wird nur selten der Fall sein.

3.2 KI-Policy für die DNB als Anbieterin und Betreiberin

Mit weiterem Fortschritt der technischen Entwicklung und der internen Projekte zu KI-Anwendungen gewann die Frage an Wichtigkeit, inwiefern die DNB selbst als Anbieterin oder Betreiberin von KI-Anwendungen tätig werden kann und soll. Eine entsprechende Richtlinie soll hierfür einen sicheren Rahmen schaffen. Noch mehr als im Bereich der Beschäftigtenperspektive soll auch die Policy für die DNB als Anbieterin und Betreiberin die technische Innovation fördern und Projekte ermöglichen, nicht verhindern. Zu diesem Zweck ist die entsprechende Richtlinie, die im Entwurf vorliegt (Stand August 2026), schlank und auf das Wesentliche reduziert gehalten.

Im Fokus stehen hier nicht die Beschäftigten, sondern die Organisation selbst. Anbieterin nach Art. 3 Nr. 3 KI-VO bzw. nachgelagerte Anbieterin (Art. 3 Nr. 68 KI-VO) kann eine Institution schon dann sein, wenn sie ein KI-System in größerem Umfang nachtrainiert/finetuned[9] oder ein System mit allgemeinem Verwendungszweck in spezifischen Kontexten einsetzt[10] und dann (und es sei auch nur intern) in Betrieb nimmt (Art. 3 Nr. 11 KI-VO) oder in Verkehr bringt bzw. dem Markt anbietet (Art. 3 Nr. 9 KI-VO). Betreiberin ist sie nach Art. 3 Nr. 4 KI-VO, wenn sie ein KI-System im eigenen Namen verwendet. Darunter sind dann auch einfache Lizenzierungen fremder Anwendungen zum Betrieb im innerdienstlichen Bereich zu verstehen. Diese Rolle nimmt eine Bibliothek also schon bei der schlichten Beschaffung einer fremden KI-Anwendung ein.

An die geschilderten beiden Rollen knüpft die KI-VO verschiedene Handlungspflichten, wobei der Großteil dieser Pflichten nur für Hochrisiko-KI relevant ist (Art. 6-49 KI-VO). Diese Kategorie von KI umfasst etwa Anwendungen im Bereich kritischer Infrastruktur oder zur Bewertung im Bildungsbereich (Art. 6 ff. KI-VO in Verbindung mit Anhang III zur KI-VO) und ist insofern für die meisten Bibliotheken irrelevant. Allenfalls bei einem Einsatz von KI bei der Personalauswahl, die ebenfalls erfasst ist, können hier Berührungspunkte vorliegen. Da solche Systeme zwar erlaubtermaßen angewendet werden dürfen, jedoch im Gegenzug sehr strenge Anforderungen an die Gestaltung des Systems und das Anbieterverhalten stellen, sind sie Einzelfälle, die von der Richtlinie explizit nicht umfasst sein sollen und daher hier ebenfalls unberücksichtigt bleiben.

Deutlich häufiger werden die Handlungspflichten einschlägig sein, die KI-Systeme unterhalb des Hochrisikobereiches betreffen. Gefordert ist hier durch Art. 50 KI-VO vor allem Transparenz gegenüber Dritten, d. h. beispielsweise die Offenlegung, dass mit einer KI und nicht mit einem Menschen interagiert wird, oder dass Bilder und Texte (v.a. Deep Fakes oder Informationen „über Angelegenheiten von öffentlichem Interesse“) KI-generiert sind (Art. 50 Abs. 4 UAbs. 1 bzw. 2 KI-VO). Zudem ist es auch hier notwendig, dass Anbietende bzw. Betreibende als Verantwortliche die datenschutzrechtlichen Grundprinzipien des Art. 5 DSGVO einhalten und damit für Rechtmäßigkeit, Zweckbin-

9 Kirschke-Biller, Jonathan, Füllsack, Anna Lena: Kommentierung zu Art. 3 KI-VO, Rn. 88.1 f, in: Schefzig, Jens, Kilian, Robert (Hg.), BeckOK KI-Recht, 01.11.2025, 6. Aufl., https://beck-online.beck.de/?vpath=bibdata%2Fkomm%2FBeckOK-KIR_6%2FEU_VO_2024_1689%2Fcont%2FBECKOKKIR%2eEU_VO_2024_1689%2eA3%2eglC%2eglIII%2egl3%2ehtm, Stand: 21.08.2026.

10 Kirschke-Biller, Jonathan, Füllsack, Anna Lena: Kommentierung zu Art. 3 KI-VO, Rn. 96, in: Schefzig, Jens, Kilian, Robert (Hg.), BeckOK KI-Recht, 01.11.2025, 6. Aufl., https://beck-online.beck.de/?vpath=bibdata%2Fkomm%2FBeckOK-KIR_6%2FEU_VO_2024_1689%2Fcont%2FBECKOKKIR%2eEU_VO_2024_1689%2eA3%2eglC%2eglIII%2egl4%2ehtm, Stand: 21.08.2026.

dung, Datenminimierung, Richtigkeit, (zeitliche) Speicherbegrenzung, Integrität und Vertraulichkeit der Daten einstehen.[11] Urheberrechtlich ist der Spielraum, wie oben bereits erläutert, noch nicht letztlich gerichtlich geklärt.[12]

Um Aufwände zu minimieren, liegt der Fokus der Richtlinie auf leicht zugänglichen Checklisten. Diese fragen bestimmte Projektaspekte ab und begleiten die Projektverantwortlichen bei der Entwicklung, dem Feintuning bzw. der Beschaffung von KI-Anwendungen. Die Durchführung soll jeweils bei der verantwortlichen Organisationseinheit liegen, während das KI-Compliance-Office bzw. die einzelnen Mitglieder eine beratende Rolle einnehmen.

Die beiden bisher vorgesehenen bzw. entwickelten Checklisten kommen dabei in zwei unterschiedlichen Phasen zum Einsatz: dem Pre-Check und dem Compliance-Check. Der sog. Pre-Check nimmt im Wesentlichen die Risikoeinschätzung vor, die KI-Anwendungen aus dem Bereich der verbotenen Praktiken (Art. 5 KI-VO) bereits frühzeitig abfangen soll. Hierbei handelt es sich z. B. um die Inbetriebnahme von Systemen, die zur unterschwelligen Manipulation von menschlichen Handlungen oder zum automatisierten sozialen Scoring von Menschen dienen sollen. Solche Anwendungen von KI sind allerdings im Bibliotheksalltag schwer praktisch vorstellbar, was wie bereits geschildert mit Abstrichen auch für die Hochrisiko-KI gilt. Ergänzend sensibilisiert der Pre-Check die Projektverantwortlichen hinsichtlich der Verarbeitung personenbezogener Daten (z. B. Notwendigkeit einer Datenschutzfolgeabschätzung) sowie der rechtmäßigen Nutzung urheberrechtlich geschützter Werke. Der Pre-Check soll bereits zum frühestmöglichen Zeitpunkt eines Projekt- bzw. Beschaffungsvorhabens durchgeführt werden. Ist der Pre-Check erfolgreich absolviert und der rechtliche Rahmen nach der KI-VO abgesteckt, beginnt die eigentliche Projektphase, d. h. die Entwicklung oder der Beschaffungsprozess.

Den weiteren Prozess bis hin zum Livegang oder Zuschlag in der Beschaffung begleitet dann der eigentliche Compliance-Check. Dieser fragt die erforderlichen technischen und organisatorischen Maßnahmen zur rechtssicheren Verarbeitung personenbezogener Daten, der Verwendung urheberrechtlich geschützter Werke, zum technischen Schutz gegen Missbrauch und externen Zugriff sowie zur Gewährleistung von Transparenz und einheitlichen Standards etwaiger externer Kooperationspartner*innen ab. Letztere können zumeist erst im Fortgang von Entwicklung bzw. Beschaffung geklärt werden. Ergibt sich hierbei durch die Art der Antwort weiterer Klärungsbedarf, werden die verantwortlichen Organisationseinheiten an die für den jeweiligen Bereich zuständigen Mitglieder des KI-Compliance-Office verwiesen. Das komplexe Geflecht „Einführung einer KI-Anwendung“ wird so in Einzelfragen zerlegt, handhabbar strukturiert und die Problemfelder werden organisiert abgearbeitet. Überdies erfolgt gewissermaßen nebenbei auch die notwendige Dokumentation der rechtlichen Prüfung und Reflexion, die in regelmäßigen Abständen durchgesehen und ggf. auch nach Inbetriebnahme der Anwendung aktualisiert werden sollte. Für diese Dokumentationserfordernisse sind sowohl Pre- als auch Compliance-Check technisch so gestaltet, dass ein Export der Ergebnisse einfach möglich ist.

11 Zu den genauen Rahmenbedingungen siehe etwa Kosler, Corvin: Datenschutzfreundliche Technikgestaltung bei KI-Systemen. Kriterien der Abwägungsentscheidung des Verantwortlichen und deren Einordnung, in: Zeitschrift für Datenschutzrecht (ZD) 2026, S. 381, 382 f.

12 Zu einem Überblick vgl. das Gutachten im Auftrag des dbv, Stieper, Malte, Verwendung von Bibliotheksbeständen für das Text- und Data-Mining, insbesondere für das KI-Training, 01.10.2025, https://www.bibliotheksverband.de/sites/default/files/2025-10/Stieper_Rechtsgutachten_KI_Training_dbv.pdf, Stand: 21.08.2026.

Für diese KI-Policy entwickelte das KI-Compliance-Office einen ersten Entwurf und stellte ihn den relevanten Stakeholdern des Hauses, insbesondere dem Zentralbereich IT, vor. So konnten insbesondere technische und weitere fachliche Aspekte angemessen berücksichtigt und in den vorfinalen Entwurf aufgenommen werden.

4. Resümee und Ausblick

KI-Compliance ist für privatwirtschaftliche Unternehmen zunächst einmal eine organisatorisch und kaufmännisch zu lösende Aufgabe, kann sich aber – einmal etabliert – als Standortvorteil erweisen. Für Bibliotheken und Informationseinrichtungen dagegen ist sie eine Notwendigkeit, die sich aus der strikten Bindung an Recht und Gesetz ergibt. Das Beispiel der DNB zeigt, wie sich eine Einzelorganisation an dieses enge Framework anpassen kann, ohne ihre Handlungsfähigkeit zu verlieren. Dies geschieht ressourcensparend, indem sie bereits vorhandene Binnenorganisationen (Justiziariat, Zuständige für Datenschutz und Informationssicherheit) im Wege einer Matrixstruktur im neuen Rahmen nutzbar macht. Überdies wird die Umsetzung bürokratiearm gestaltet, indem die Mitarbeitenden einerseits kompetenzgerecht in die Pflicht genommen werden, andererseits aber diese Verantwortung ohne überflüssige Berichtspflichten und mit einem Minimum an Dokumentationsaufwand erfüllt werden kann. Dabei muss klar sein, dass die organisatorische Einbindung neuer Technologien niemals ein Projekt mit einem festen Endpunkt sein kann. Die Arbeit des KI-Compliance-Office an internen Regelwerken ist deshalb an dieser Stelle nicht abgeschlossen. Nicht nur verstehen sich alle Policys erklärtermaßen als „lebende und lernende" Dokumente. Auch Rechtsprechung und Gesetzgebung als Handlungsrahmen entwickeln sich stetig weiter. Zuletzt wurde etwa die KI-Verordnung durch die Digital-Omnibus-Verordnung zur KI („Omnibus on AI") [13] novelliert und z. B. die Fristen für die Umsetzung einzelner Regelungen großzügiger gestaltet. Durch die Bündelung rechtlicher und sicherheitsbezogener Kompetenz und einen strukturierten, zugleich die Umstände des Einzelfalls angemessen berücksichtigenden Prozess lässt sich die rasante technische Entwicklung sicher nutzen und flexibel beherrschen. Nicht jede Bibliothek wird den entsprechenden Aufwand selbst stemmen können – umso wichtiger ist die Kooperation zwischen den Einrichtungen, beispielsweise durch einen Austausch von Best-Practice-Beispielen und internen Regelungen.

Simon Herrmann, Deutsche Nationalbibliothek, Frankfurt am Main, https://orcid.org/0000-0002-3083-8758
Christoph Wohlstein, Deutsche Nationalbibliothek, Frankfurt am Main, https://orcid.org/0009-0003-0428-248X

Zitierfähiger Link (DOI): https://doi.org/10.5282/o-bib/6311

Dieses Werk steht unter der Lizenz Creative Commons Namensnennung 4.0 International.

13 Diese Regelung ist Teil eines größeren Pakets von Vereinfachungen und Klarstellungen der EU-Digitalgesetzgebung; VERORDNUNG (EU) 2026/1744 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 8. Juli 2026 zur Änderung der Verordnungen (EU) 2024/1689, (EU) 2018/1139 und (EU) 2023/1230 im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz (Digital-Omnibus-Verordnung zur KI), https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32026R1744, Stand: 21.08.2026.