Rundfunkdatenschutzkonferenz
RDSK
ARD | ZDF | Deutschlandradio

Orientierungshilfe zum datenschutzkonformen Einsatz von KI im öffentlich-rechtlichen Rundfunk

(Version 2.1 - Stand: September 2024)

Diese Orientierungshilfe der RDSK soll über die (datenschutz-)rechtlichen Hintergründe und Maßgaben beim Einsatz von KI im öffentlich-rechtlichen Rundfunk informieren und über Risiken aufklären. Die sich daraus ergebenden Konsequenzen werden erläutert und konkrete Handlungsanweisungen bzw. Vorgaben (je nach Einsatzgebiet) entwickelt, sowie Fragen formuliert, die vor und bei dem Einsatz von KI zu stellen sind. Aufgrund der dynamischen Entwicklung im Bereich von KI wird diese Orientierungshilfe kontinuierlich überarbeitet.

I. Ausgangspunkt/Fragestellung

Künstliche Intelligenz bzw. maschinelles Lernen ist eine immense Herausforderung für den Datenschutz. Welche Besonderheiten ergeben sich darüber hinaus für den öffentlich-rechtlichen Rundfunk?

II. Hintergrund

1. Allgemeine Funktionsweise von KI

Die Anwendungen lernen aus der Kommunikation und können - neben dem Erkennen und Sortieren bestimmter Inhalte - Texte (z.B. journalistischer oder wissenschaftlicher Natur) oder auch Software-Code generieren, Präsentationen, Bilder und Videos produzieren (Stichwort: Deepfakes und KI-Collagen) oder auch menschliche Stimmen künstlich erzeugen und Musikstücke herstellen.

Dafür greifen viele Anwendungen auf Quellen aus dem Internet zurück (etwa soziale Medien, Online-Foren, Zeitungsartikel und Bücher).

KI ist mithin nicht nur datenbasiert, sondern funktioniert ausschließlich mit der Verarbeitung von Daten. Sind diese Daten personenbezogen, gelten die Regelungen der europäischen Datenschutzgrundverordnung (DSGVO) und weitere für den Rundfunk einschlägige Datenschutzvorschriften.

2. EU KI-Verordnung (2024)

Ein neuer Rechtsrahmen in der EU für die einheitliche Regulierung Künstlicher Intelligenz wurde am 21.05.2024 durch den Rat der Europäischen Union mit der sogenannten KI-Verordnung[1] (engl. AI Act) verabschiedet und trat am 01.08.2024 in Kraft.

[1] https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_DE.pdf

Der in der KI-VO verwendete Ausdruck **KI-System** wird in Art. 3 Nr. 1 KI-VO definiert und bezeichnet

> *„[…] ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können."*

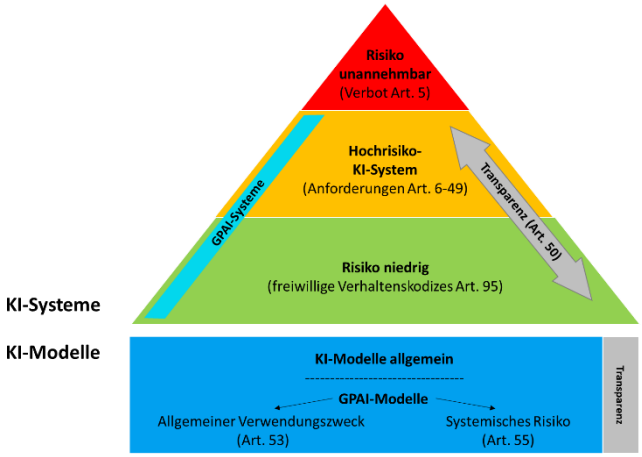
Unter dem Begriff KI-System ist damit das vom Endnutzer nutzbare Produkt zu verstehen (z.B. ChatGPT oder Microsoft Copilot)[2]. Ein **KI-Modell**, das in der KI-VO nicht definiert wird, meint die KI selbst, also den programmierten und selbst lernenden Algorithmus (z.B. GPT-4).

Die KI-Verordnung (KI-VO) verfolgt einen risikobasiertem Ansatz (d. h. die Pflichten für ein KI-System richten sich nach dem individuellen Einsatzszenario[3]) und ist weltweit das erste umfassende Regelwerk zu KI[4]. Die DSGVO wird in ihrem Regelungsgehalt jedoch nicht beschränkt. Für die journalistische Datenverarbeitung enthält die KI-VO keine privilegierenden Vorschriften – d. h., die Regelungen sind auch im journalistischen Bereich zu beachten.

Je nach Risiko, das vom jeweiligen KI-System ausgeht, legen die Vorschriften Verpflichtungen für Anbieter und Nutzer fest.

Unterschieden werden KI-Systeme in grundsätzlich **drei Risikoklassen**:

1. **Unannehmbares Risiko**[5] (verboten),
2. **Hochrisiko-KI-Systeme**[6] (strenge Anforderungen),
3. **Niedriges Risiko**
   a) grundsätzlich keine speziellen rechtlichen Anforderungen[7]
   b) Sonderfall: KI-Modelle mit allgemeinem Verwendungszweck – „GPAI" (Transparenzanforderungen)



Unterhalb der Hochrisiko-Grenze enthält die KI-VO konkrete Regelungen für KI-Modelle mit allgemeinem Verwendungszweck (Art. 51. ff. KI-VO), auch **General Purpose AI (GPAI)** genannt, darunter werden KI-Modelle wie GPT-4, DALL-E, Google Gemini oder Midjourney 5.1. gefasst, die in der Lage sind, ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen. Für solche KI-Modelle und damit verbundene KI-Systeme wird in der Regel ein niedriges bzw. begrenztes Risiko gesehen. Es gelten (jedoch lediglich für die Anbieter [!],

---

[2] Bomhard/Siglmüller, AI Act – das Trilogergebnis, RDi 2024, 45 Rn. 24
[3] Bomhard/Siglmüller, AI Act – das Trilogergebnis, RDi 2024, 45 Rn. 23
[4] https://www.europarl.europa.eu/topics/de/article/20230601STO93804/ki-gesetz-erste-regulierung-der-kunstlichen-intelligenz
[5] Art. 5 KI-VO – Beispiele: KI-Systeme, die gezielt menschliche Schwächen ausnutzen (z.B. Alter, Behinderung, bestimmte soziale oder wirtschaftliche Situation), Social Scoring, Profiling im Hinblick auf Straffälligkeit, Erweiterung von Datenbanken zur Gesichtserkennung durch Scraping, Ableitung von Emotionen am Arbeitsplatz, bestimmte Biometrische Kategorisierungssysteme, Echtzeit-Fernidentifizierungssysteme in öffentlichen Räumen)
[6] Art. 6 und Annex III der KI-VO – Beispiele: bestimmte Biometrische Identifizierungs- oder Kategorisierungssysteme (Gesichtserkennung, Stimmerkennung, Emotionserkennung oder Verhaltensanalyse), KI-Systeme in sicherheitskritischen Bereichen (z.B. Wasser-, Gas- Wärme- und Stromversorgung), bewertende KI-Systeme in bestimmten Bereichen – in der Regel generative KI-Systeme (z.B. Bewertung von Bewerbern im Personalmanagement, Leistungen von Schülern und Auszubildenden, Bewertung der Kreditwürdigkeit), KI-Systeme im Zusammenhang mit Wahlen
[7] Anbieter solcher Systeme sollen Verhaltenskodizes erstellen und die Regelungen für Hochrisiko-KI-Systeme freiwillig anwenden (Art. 95 KI-VO)

nicht für die Anwender) die speziellen Transparenzanforderungen aus Art. 53 KI-VO (z.B. Kennzeichnungspflichten) und bei systemischem Risiko[8] weitergehende Pflichten aus Art. 55 KI-VO (so z. B. auch bei GPT-4 oder Gemini). Sofern eine GPAI ohne systemisches Risiko vom Anwender in einem als Hochrisiko-Bereich (im Sinne der KI-VO[9]) eingestuften Anwendungsgebiet zum Einsatz kommt, geht die Verwendung als Hochrisiko-System mit entsprechenden Pflichten auch für den Anwender einher.

In vollem Umfang anwendbar wird die KI-VO erst nach einer Umsetzungszeit von 24 Monaten nach dem Inkrafttreten, also ab 01.08.2026. Das Verbot von KI mit unannehmbaren Risiken gilt jedoch bereits sechs Monate nach Inkrafttreten ab 02.02.2025, die Regelungen zu KI mit allgemeinem Verwendungszweck (z. B. Transparenzanforderungen) gelten ab 02.08.2025. Eine Ausnahme bilden die Einstufungsvorschriften für Hochrisiko-KI-Systeme (Art. 6 Abs. 1 KI-VO), die erst nachträglich ab 02.08.2027 Geltung entfalten.

Auch außerhalb der EU werden Versuche zur Regulierung von KI diskutiert. Die „Internationale Datenschutzkonferenz“ (Global Privacy Assembly – GPA) hat 2021 eine ständige Arbeitsgruppe gebildet, die sich mit ethischen Fragen und speziell dem Thema Datenschutz im Bereich künstlicher Intelligenz befasst („Working Group on Ethics and Data protection in Artificial Intelligence“[10]).

III. Datenschutzrechtliche Grundlagen

Die DSGVO spricht an keiner Stelle ausdrücklich von KI, jedoch ist Erwägungsgrund 15 DSGVO zu entnehmen, dass der Schutz natürlicher Personen technologieneutral und unabhängig von einer verwendeten Technologie sein soll. KI-Systeme als Technologie sind für deren Funktionieren auf die zugeführten Daten (insbesondere Trainingsdaten) angewiesen.[11]

Von datenschutzrechtlicher Bedeutung ist demnach die Verarbeitung personenbezogener Daten zum Zweck des Trainings und der Erzeugung einer KI-Anwendung. Daneben ist die Anwendung einer bereits trainierten KI auf einen gewissen Sachverhalt relevant.

Für **Verarbeitungstätigkeiten mit Personenbezug** (Definition: vgl. Art. 4 Nr. 2 DSGVO), bei denen Komponenten der Künstlichen Intelligenz (KI-Komponenten) zum Einsatz kommen, gelten – wie bei allen anderen Verarbeitungen auch – die in der DSGVO formulierten Grundsätze (vgl. Art. 5 Abs. 1 DSGVO[12]).

Zunächst ist erforderlich, den **Zweck des Einsatzes** eines KI-Systems und die Notwendigkeit der damit einhergehenden Datenverarbeitung personenbezogener Daten so eng wie möglich zu beschreiben.

Wichtig ist insbesondere die Herstellung der Prüfbarkeit einer Verarbeitungstätigkeit (**Transparenz**).[13] Dazu gehören die Erstellung und Anpassung von Datenschutzerklärungen und Einwilligungstexten. Ebenso sind

[8] Gemäß Art. 51 KI-VO, wenn ein Modell über „hohe Wirkungskapazitäten“ verfügt, z. B. eine bestimmte technische Schwelle an Rechenoperationen erreicht (trainiert mit einer Gesamtrechenleistung von mehr als 10^25 FLOPs) oder vorhersehbare negative Folgen (nach Festlegung der EU-Kommission oder nach Warnmeldung eines wissenschaftlichen Gremiums) hat. Hintergrund ist auch, dass die Fähigkeiten der Modelle oberhalb des Schwellenwerts noch nicht ausreichend verstanden werden (siehe: https://ec.europa.eu/commission/presscorner/detail/de/QANDA_21_1683)

[9] siehe Art. 6 KI-VO und Anhang III zur KI-VO

[10] Report 2023: https://globalprivacyassembly.org/wp-content/uploads/2023/10/8.-Ethics_and_Data_Protection_in_AI_Working_Group_2023-For_circulation_to_GPA.pdf

[11] Schürmann, Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz, in: ZD 2022, 316

[12] 1. Rechtmäßigkeit, Fairness und Transparenz; 2. Zweckbindung, 3. Datenminimierung, 4. Richtigkeit, 5. Speicherbegrenzung, 6. Integrität und Vertraulichkeit

[13] Ausführlich auch mit Übersicht zu entsprechenden TOM: Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen vom 06.11.2019: https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf

technische und organisatorische Maßnahmen nach Art. 32 DSGVO zu ergreifen und ggf. Auftragsverarbeitungsverträge zu schließen. Schließlich können Spezifikationen[14], Dokumentationen, sowie insbesondere aktive Tests der KI-Systeme oder -Komponenten notwendig werden.

Wie stets, muss die Verarbeitung von personenbezogenen Daten zudem den Anforderungen nach Art. 6 Abs. 1 DSGVO entsprechen, d. h. es muss eine **Rechtsgrundlage** für die konkrete, mit dem Einsatz der KI verbundenen, Datenverarbeitung gefunden werden. Klarstellend: Die Erfüllung der Anforderungen aus der KI-VO ist zu beachten, stellt aber keine datenschutzrechtliche Rechtsgrundlage im Sinne des Art. 6 Abs. 1 DSGVO dar.

Relevant für die datenschutzrechtliche Prüfung ist die **Unterscheidung von offenen und geschlossenen KI-Systemen**. Geschlossene Systeme (z.B. On-Premise Anwendungen) verarbeiten Daten nur in einer begrenzten technisch abgeschlossenen Umgebung (dies kann auch eine abgeschlossene Cloud-Infrastruktur sein, z.B. Private-Cloud). Ein Zugriff auf die im geschlossenen System verarbeiteten Daten durch das frei zugängliche Internet ist ausgeschlossen. Damit fließen die Daten nicht in das allgemeine Training des KI-Systems mit ein, lediglich ein Training innerhalb des geschlossenen Systems ist möglich.
Offene Systeme sind in der Regel cloudbasiert und werden über das frei zugängliche Internet betrieben und durch einen unbestimmten Personenkreis trainiert. Das Risiko, das personenbezogene Daten dann zu anderen Zwecken weiterverarbeitet und an anderer Stelle offengelegt werden, ist mangels Kontrolle und Transparenz hoch.

Wenn die Auswirkungen KI-typischer automatisierter Entscheidungen oder Entscheidungsvorbereitungen voraussichtlich hohe Risiken für die Rechte und Freiheiten natürlicher Personen zur Folge haben, muss eine **Datenschutz-Folgenabschätzung (DSFA)** gem. Art. 35 DSGVO durch den Verantwortlichen durchgeführt werden. Liegt eine Hochrisiko-KI im Sinne der KI-VO vor, ist davon auszugehen, dass auch ein hohes Risiko im Sinne der DSGVO vorliegt. Damit ist in solchen Fällen eine Datenschutz-Folgenabschätzung durchzuführen. KI-Systeme, die gemäß der KI-VO nur ein geringes Risiko aufweisen, sind aber nicht automatisch nach datenschutzrechtlichem Verständnis frei von hohen Risiken. Hier ist deshalb sehr genau zu prüfen, ob gemäß Art. 35 DSGVO eine Datenschutz-Folgenabschätzung durchzuführen ist. Insbesondere bei General Purpose AI (GPAI) mit systemischem Risiko (siehe auch Fußnote 8) ist die Erforderlichkeit einer Datenschutz-Folgenabschätzung gegeben, Ausnahmen bilden geschlossene KI-Systeme, in denen sich das systemische Risiko des KI-Modells nicht in der Anwendung auswirkt. Dies sollte im Einzelfall geprüft und begründet werden (siehe dazu auch Kapitel II. „Hintergrund, S. 3 oben)“.

In diesem Zusammenhang findet sich in Art. 27 KI-VO eine Sonderregelung für Einrichtungen des öffentlichen Rechts (wozu auch die öffentlich-rechtlichen Rundfunkanstalten zu zählen sind). Danach müssen diese Einrichtungen vor Inbetriebnahme von Hochrisiko-KI-Systemen eine **Grundrechte-Folgenabschätzung** durchführen, die ausdrücklich gemäß Art. 27 Abs. 4 KI-VO ergänzend neben einer Datenschutz-Folgenabschätzung steht. Die allgemeinere Grundrechte-Folgenabschätzung stellt auf alle Rechte und Freiheiten der betroffenen Personen ab, wohingegen die DSFA lediglich an die Verarbeitung der personenbezogenen Daten als gefährdende Handlung anknüpft.

[14] Anpassungen zur datensparsamen Nutzung in den Einstellungen der genutzten KI-Systeme oder die Hinterlegung von Beschränkungen in robots.txt-Dateien zur Steuerung von Informationen, die von Suchmaschinen-Crawlern gelesen werden.

IV. Risiken

Derzeit ergeben sich im Umgang mit Anwendungen der KI regelmäßig insbesondere folgende Risiken und Probleme:

1. Mangelnde Transparenz: Aus welchen Quellen stammen die Daten, auf die die Systeme zurückgreifen?
2. Mangelnde Informationen: Auf welcher Rechtsgrundlage werden die Daten verarbeitet?
3. Werden die Informationspflichten von betroffenen Personen erfüllt?
4. Können betroffene Personen ihre Rechte auf Auskunft, Berichtigung und Löschung wirksam ausüben?
5. Ist die Sicherheit der verarbeiteten Daten gewährleistet?
6. Wo werden die Daten verarbeitet (ggf. unzureichende Datenschutzstandards in Ländern außerhalb der EU)?
7. An welche weiteren Unternehmen werden die Daten weitergegeben?
8. Werden die Daten für andere, nicht vom Nutzer festgelegte Zwecke (z.B. Training der KI) genutzt?
9. (Wie) Werden Daten von Kindern geschützt?

Die hier beschriebenen Risiken betreffen zunächst Anbieter von Systemen, die auf KI basieren. Probleme ergeben sich jedoch auch aus Perspektive der Rundfunkanstalten oder Unternehmen, die die KI nutzen möchten.

V. Medienprivileg (gilt auch im Hinblick auf durch den öffentlich-rechtlichen Rundfunk eingesetzte KI)

Unternehmen und Rundfunkanstalten, die sich auf das Medienprivileg berufen können, werden Ausnahmen von datenschutzrechtlichen Vorschriften gewährt. Insbesondere muss für die redaktionelle Tätigkeit keine datenschutzrechtliche Einwilligung eingeholt werden, wenn Daten zu einer Person zu Recherchezwecken verarbeitet werden.

Allerdings verpflichten die Regelungen des Medienstaatsvertrags zur **Einhaltung des Datengeheimnisses**, wonach personenbezogene Daten nicht zu anderen als journalistischen Zwecken verarbeitet werden dürfen. Auch gilt insbesondere der **Grundsatz der Vertraulichkeit und Integrität** zur Gewährleistung der **Datensicherheit**. In diesem Zusammenhang müssen die Verantwortlichen geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten, z. B. vor unbefugter oder unrechtmäßiger Verarbeitung und Weiterverarbeitung durch die KI treffen. Dies ist ggf. auch vertraglich sicher zu stellen (siehe dazu auch Kapitel VI. „Verantwortlichkeit“).

VI. Verantwortlichkeit

Aus datenschutzrechtlicher Sicht ist die Frage zu klären, wer für die Datenverarbeitung im Einzelnen verantwortlich ist. Es kommen in Betracht die Auftragsverarbeitung nach Artikel 28 DSGVO, die gemeinsame Verantwortung nach Artikel 26 DSGVO oder aber die getrennte Verantwortung.

1. Auftragsverarbeitung

Im Normalfall wird bei der Beauftragung einer „Software as a Service“ ein Auftragsverarbeitungsvertrag (AVV) abgeschlossen. Hintergrund ist, dass der Dienstleister (hier der KI-Anbieter) weisungsabhängig agiert, die Daten ausschließlich zu den vereinbarten Zwecken verwendet und somit die Verantwortung

für die Datenverarbeitung vollständig beim Auftraggeber (hier der Rundfunkanstalt) verbleibt. Die Anforderungen von Artikel 28 DSGVO an einen AVV sind zu beachten.

Open AI als Anbieter von ChatGPT ist der Auffassung, Auftragsverarbeiter zu sein, und stellt im Falle eines zahlungspflichtigen Abonnements einen AVV bereit, der auch nicht abgeändert werden darf – so zumindest die Maßgabe von Open AI. Auch andere Muster werden nicht akzeptiert.[15]

Es gibt Bedenken, dass die vom Auftraggeber in die KI eingespeisten Daten nicht nur auftragsgemäß, sondern auch zu eigenen davon getrennten Zwecken verarbeitet werden. Dies wäre mit europäischem Recht nicht zu vereinbaren. Wegen der nicht hinreichenden Transparenz der Datenverarbeitung innerhalb der Künstlichen Intelligenz ist dieses Risiko zumindest nicht ausgeschlossen.

2. Gemeinsame Verantwortung

Sollten Auftraggeber und Auftragnehmer eine gemeinsame Entscheidung über Zwecke und Mittel der Datenverarbeitung treffen, so ist eine Joint-Controller-Vereinbarung abzuschließen. Dies ist insbesondere dann der Fall, wenn man sich gemeinsam für eine Datenverarbeitung entscheidet. Dies ist beim Einsatz von KI-Systemen nicht der Regelfall.

3. Getrennte Verantwortung

Im dritten und letzten Fall wären die Verantwortungssphären getrennt, d.h. dass die Rundfunkanstalt die eingesetzten Daten und die damit verbundene Verarbeitung vollständig und allein verantwortet, ebenso aber auch das KI-Unternehmen die Datenverarbeitung zu eigenen Zwecken. Das Problem hier besteht darin, dass die Daten, die in das System eingespeist werden von der Rundfunkanstalt stammen und damit eine Rechtsgrundlage für die Übermittlung der Daten an die KI betreibende Unternehmen vorhanden sein müsste. Dies ist stets einzelfallabhängig, aber im Regelfall nicht gegeben.

Im Regelfall ist daher anzuraten, lediglich auf Basis einer rechtlich einwandfreien Auftragsverarbeitungsvereinbarung KI einzusetzen. Dies gilt in erster Linie für Daten **im nichtjournalistischen Bereich**, denn für die Verarbeitung von journalistischen Daten durch Dritte ist der Abschluss eines AVVs wegen des Medienprivilegs (siehe dazu Kapitel V.) nicht vorgeschrieben. Dabei ist jedoch zu beachten, dass aufgrund der strengen Zweckbindung journalistischer Daten ebenso auszuschließen ist, dass Dritte diese Daten für eigene Zwecke (hier: der KI-Anbieter) verwenden. **Daher ist auch für KI-Anwendungen, die für journalistische Zwecke eingesetzt werden, der Abschluss eines entsprechenden Vertrages, der die Sicherheitsrisiken in den Blick nimmt und regelt (Festlegung technischer und organisatorischer Maßnahmen), ausdrücklich zu empfehlen.**

Sollten sich im Prozess Anhaltspunkte ergeben, dass Daten nicht zweckgebunden und vertragsgemäß durch den KI-Anbieter verarbeitet werden, darf die KI bis zur Klärung nicht genutzt werden.

[15] „Unfortunately, we are unable to review or sign DPAs provided by our customers or customize our DPA on a case by case basis."

VII. Chancen

Technologische Entwicklungen – namentlich Digitalisierungsprozesse – haben die Produktion und Nutzung von Medieninhalten seit geraumer Zeit verändert. Damit hat sich auch die journalistische Arbeit verändert. Die Nutzung von KI für Recherche, Aufbereitung und Erstellung medialer Inhalte muss dem technologischen Fortschritt gerecht werden, ohne dass der verfassungsrechtliche Auftrag gefährdet wird.

> *„KI kann zur Stärkung von Medienvielfalt in der Produktion führen. KI kann aber auch eingesetzt werden, um mit Sparzwängen in Redaktionen umzugehen und den Trend weg von zeit- und arbeitsintensivem Investigativ-Journalismus hin zu Formaten zu verstärken, die darauf ausgelegt sind, schnell Aufmerksamkeit zu erlangen. Zusätzlich können KI-Technologien auch zur Manipulation öffentlicher Diskurse genutzt werden, da sie neue Möglichkeiten bieten, mit geringem Aufwand und geringen Kosten Medieninhalte mit hoher Qualität zu fälschen oder zu manipulieren.“*[16]

Hinsichtlich der Erstellung neuer Programmangebote besteht mithin grundsätzlich eine Offenheit gegenüber dem Einsatz von KI, da Medienproduktion, redaktionelle Arbeit und Programmangebot ineinandergreifen. Das öffentlich-rechtliche Profil muss dabei jedoch gewahrt bleiben. KI darf journalistisches Arbeiten nicht ersetzen, sondern kann dieses ggf. unterstützen.

VIII. Konsequenzen für den Einsatz von KI im öffentlich-rechtlichen Rundfunk nach aktueller Einschätzung

Für die Informationsbeschaffung, die Produktion von Programmangeboten und auch deren inhaltliche Ausgestaltung sind für KI die unter „Risiken“ aufgeführten Fragen zu beantworten, die Maßgaben der KI-Verordnung zu beachten und verbleibende Rechtsrisiken zu bewerten. Empfohlen wird eine wirksame Selbstregulierung bzw. die Weiterentwicklung eines journalistischen Verhaltenskodex. Dienstanweisungen der einzelnen Rundfunkanstalten, die auch den Einsatz von KI umfassen, sind zu beachten.

Um einen Einsatz von KI rechtssicher zu ermöglichen, ist auch unter Beachtung der Vorgaben aus den Kapiteln III. und VI. Folgendes zu beachten:

1. Redaktionelle Zwecke

- KI-Anwendungen (auch offene Systeme) können redaktionelles Arbeitsmittel und/oder Berichtsgegenstand sein. Für die Nutzung zu beiden Zwecken werden regelmäßig personenbezogene Daten von den Anwendungen verarbeitet (z. B. E-Mail-Adressen, aber auch Protokoll- und Nutzungsdaten, Benutzerinhalte und Kommunikationsinformationen (Namen)). Daher ist darauf zu achten, dass Beschäftigte möglichst wenig Daten preisgegeben – Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO).
- Bei Nutzung offener Systeme ist nach Möglichkeit die Nutzung der Daten für das Training der KI auszuschließen (z. B. in den Einstellungen der jeweiligen Anwendung).
- Die eingesetzten Systeme dürfen die Einhaltung des Datengeheimnisses nicht gefährden und den Grundsatz der Vertraulichkeit und Integrität zur Gewährleistung der Datensicherheit nicht verletzen. Die in die offenen KI-Anwendungen eingespeisten Inhalte dürfen daher nicht vertraulich sein. D. h.:

[16] Deutscher Bundestag, Drucksache 19/23700, Bericht der der Enquete-Kommission Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale, abrufbar unter https://dserver.bundestag.de/btd/19/237/1923700.pdf#page447

  - Vertrauliche (redaktionelle) Informationen und Redaktionsgeheimnisse dürfen nicht in offene KI-Anwendungen im Internet eingespeist werden.
  - Der Informantenschutz muss stets gewahrt bleiben.
- Beim Einsatz von KI sind die Programmgrundsätze zu wahren. Auch bei KI-generierten Programmangeboten gilt die journalistische Sorgfaltspflicht.
- Die Persönlichkeitsrechte betroffener Personen sind auch beim Einsatz von KI zu wahren.
- Kinder genießen besonderen Schutz. Dieser muss auch beim Einsatz von KI beachtet werden.
- Der Verantwortliche sollte prüfen, ob Angebote, die mithilfe von KI ganz oder teilweise erstellt werden, entsprechend gekennzeichnet werden.
- Die von KI-Anwendungen verarbeiteten Daten können urheberrechtlich geschützt sein. Die Vorgaben des Urheberrechts gelten auch beim Einsatz von KI.

2. Unternehmensinterne Zwecke

- Hinsichtlich des diesbezüglichen Einsatzes von KI ist zu beachten, dass interne, vertrauliche und streng vertrauliche Informationen nicht in offene KI-Systeme eingespeist werden dürfen.
- Daten aus einem Intranet, interner Schriftverkehr, Korrespondenzen mit Geschäftspartnern, Beschäftigtendaten (etwa Daten zu Einkommen, Bewerbungsunterlagen, Arbeitszeugnisse, Gesundheitsdaten, Daten für die interne Personalplanung) oder auch Geschäftsgeheimnisse (z. B. streng vertrauliche Revisionsberichte) können aufgrund der benannten Risiken nicht mit offenen KI-Systemen verarbeitet werden.
- Offene KI als Arbeitsmittel für unternehmensinterne Zwecke kann mithin nur für solche Informationen eingesetzt werden, die ohnehin öffentlich sind (dies sind z. B. öffentlich erreichbare Internetseiten, öffentlich zugängliche Verzeichnisse oder andere öffentlich zugängliche Quellen (Pressemitteilungen, frei zugängliche Medienangebote)).
- An eine automatisierte Anbindung bzw. voreingestellte technische Verknüpfung von bestimmten Tools mit anderen bereits eingesetzten Anwendungen (z. B. bei Microsoft365-Produkten) sind besonders hohe Anforderungen zu stellen. Voreingestellte technische Verknüpfungen sollten grundsätzlich deaktiviert werden, um vor einer sonst ggf. automatisierten Implementierung eine sorgfältige Prüfung zu ermöglichen.
- Der Einsatz von geschlossenen KI-Anwendungen (z.B. On-Premise oder Private-Cloud) ist vorzugswürdig, weil solche Systeme nur für die Mitarbeitenden der Rundfunkanstalten zugänglich sind und keine Schnittstelle zum Internet haben. Die bei Anwendung eingegebenen oder entstehenden Daten werden vom Anbieter der KI damit nicht zum Training der KI verwendet.

Weitere Literatur zum Thema:

- Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ der DSK vom 6. Mai 2024
- EU-Kommission, Künstliche Intelligenz – Fragen und Antworten (Stand: 12.12.2023)

Anhang: Zusammenfassung und Checkliste für den datenschutzkonformen Einsatz von KI

IX. Anhang: Zusammenfassung und Checkliste für den datenschutzkonformen Einsatz von KI

1. In welchen Bereichen wird KI eingesetzt oder könnte KI eingesetzt werden (Zweckbestimmung)?

- Journalistisch-redaktioneller Bereich: z.B. Generierung von Bild-/Textmaterial, Audio Mining (Transkription von Audiodaten),
  Zum journalistischen Bereich im weiteren Sinne gehören auch:
  - Produktion (fiktional): z.B. Generierung von Bildmaterial, Farbkorrektur, visuelle Effekte
  - Technik-Bereich: z.B. Erstellung von Programmiertexten, Recherche bei technischen Problemen
- Unternehmensinterner Bereich/Verwaltungsbereich: z.B. Software zur Überprüfung von Prozessen, Generieren von Schriftverkehr, Diktiersoftware, Personalplanung

2. Was muss vor dem Einsatz eines KI-Tools geprüft werden?

Bereits bei der Marktsondierung und späteren Produktauswahl müssen diese Fragen geklärt werden:

- Ist der Anbieter vertrauenswürdig (wird transparent informiert)?
- Aus welchen Daten-Quellen bedient sich die KI? / Mit welchen Daten wird/wurde die KI trainiert?
- Wo wird die KI betrieben (Server-Standort)?
- Handelt es sich um ein geschlossenes oder offenes KI System?
- Gibt es die Möglichkeit über die Einstellungen der Anwendung die verarbeiteten Daten vom Training einer offenen KI auszuschließen (vorzugswürdig)?
- Ist die Sicherheit der Daten gewährleistet?
- Ist die Datenverarbeitung rechtlich zulässig (Rechtsgrundlage nach der DSGVO)?
- Besteht ein hohes oder systemisches Risiko (gemäß KI-Verordnung) für die Rechte und Freiheiten natürlicher Personen (z. B. durch Verarbeitung vertraulicher oder sensibler Daten)?
  - Wenn ja muss eine Datenschutz-Folgenabschätzung (DSFA) gem. Art. 35 DSGVO durchgeführt werden. Besteht Unsicherheit über das tatsächliche Risiko, ist im Zweifel eine DSFA angezeigt.
  - Zusätzlich müssen Einrichtungen des öffentlichen Rechts (auch die Rundfunkanstalten und Körperschaften) vor Inbetriebnahme von Hochrisiko-KI-Systemen gem. Art. 27 KI-VO eine Grundrechte-Folgenabschätzung durchführen.
- Gibt es einen Auftragsverarbeitungsvertrag (AVV) mit dem Dienstleister?
- Werden Betroffene vor der Verarbeitung ihrer Daten ausreichend informiert?
- Haben Betroffene die Möglichkeit, ihre Betroffenenrechte wahrzunehmen?

3. Welche Besonderheiten gelten im journalistischen Bereich durch das Medienprivileg?

- Datenschutz gilt im Programmbereich nur eingeschränkt (Rundfunkfreiheit).
- Daten für journalistische Zwecke dürfen auch ohne datenschutzrechtliche Rechtsgrundlage verarbeitet werden, auch in der KI.
- Die betroffenen Personen müssen nicht einwilligen.
- Dennoch sind Datengeheimnis, Redaktionsgeheimnis und Informantenschutz (Datenklassifizierung) und Maßgaben der Datensicherheit zu wahren, der KI-Dienstleister muss diese vertraglich gewährleisten können (Vertrag ggf. in Anlehnung an einen AVV).

4. Was ist beim KI-Einsatz im unternehmensinternen Bereich/Verwaltungsbereich zu beachten?

- Betriebliche IT- und Datenschutzregelungen sind einzuhalten.
- Datenklassifizierung: Es dürfen keine internen und vertraulichen Daten in offenen KI-Systemen verarbeitet werden (z. B. Gehaltsdaten, Bewerbungen, Personalunterlagen).
- Lokale KI-Lösungen (geschlossene Systeme) können diese Lücke schließen.

5. Welche Stellen sollten bei der geplanten Einführung einer KI-Lösung einbezogen werden (abhängig von der konkreten Aufgabenverteilung in der jeweiligen Rundfunkanstalt)?

- Verantwortliche Führungskraft (als verantwortliche Stelle für die spätere Datenverarbeitung)
- Bereichsleitung / Geschäftsführung (sofern bereichs-/unternehmensweite Einführung geplant ist)
- Datenschutzbeauftragte/r
- IT-Sicherheitsbeauftragte/r
- Ggf. Interessenvertretungen (wenn Mitbestimmung erforderlich ist)