„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht

1/2026
Januar 2026

Wenn die Bibliothek mitredet

Eine öffentliche Bibliothek versah Bücher ihrer Sammlung mit einem inhaltlichen Warnhinweis – durfte sie das?

Von Nikolaus von Bernuth, Berlin

In einer Eilentscheidung hat das Oberverwaltungsgericht (OVG) Münster dem Antrag eines Autors stattgegeben, der sich durch eine öffentliche Bibliothek in seinen Grundrechten verletzt sah. Die Bibliothek hatte distanzierende Hinweise an einem Buch des Autors angebracht. In der Entscheidung zeigen sich komplexe Fragen zu Funktion und Auftrag öffentlicher Bibliotheken – und zu ihren Wechselwirkungen mit den Grundrechten. Das OVG Münster sah durch den Hinweis die Grundrechte des Autors verletzt. Von besonderem Interesse ist sie gerade für den Betrieb öffentlicher, auch wissenschaftlicher Bibliotheken.

I. Sachverhalt

Die Stadtbibliothek Münster hat etwa 350.000 Werke in ihrem Bestand. Zwei ihrer Werke hatte sie – nachdem es Beschwerden gegeben hatte – mit einem Warnhinweis versehen. Der Hinweis lautete:
„Dies ist ein Werk mit umstrittenem Inhalt. Dieses Exemplar wird aufgrund der Zensur-, Meinungs- und Informationsfreiheit zur Verfügung gestellt."

Mit dem Hinweis nahm die Bibliothek auf Inhalte in den Büchern Bezug, die für mehrfache Beschwerden gesorgt hatten. Eines der Bücher enthielt die Leugnung historischer Tatsachen wie etwa des Atombombenabwurfs über Hiroshima und Nagasaki.[1] Der Autor eines dieser Werke ging gerichtlich dagegen vor. Er verlangte im Eilverfahren, dass die Bibliothek diesen Hinweis aus seinen Büchern entfernt. Während das Verwaltungsgericht (VG) Münster[2] seinen Antrag noch ablehnte, gab ihm das Oberverwaltungsgericht (OVG) Münster[3] im Eilverfahren recht.

Der Fall wirft grundsätzliche Fragen auf. Diese betreffen zum einen Funktion und Handlungsspielräume öffentlicher Bibliotheken, zu denen auch die Bibliotheken an öffentlichen Hochschulen und Forschungseinrichtungen zählen. Darüber hinaus ergeben sich auf rechtlicher Ebene Fragen, die die Geltung und Reichweite der Grundrechte im Bibliothekskontext betreffen. Um den Fall hat sich daher auch eine verfassungsrechtliche Diskussion entwickelt. Das OVG Münster konnte diese grundlegenden Fragen im vorliegenden Eilverfahren nur überblicksartig prüfen, doch bereits diese Überlegungen lohnen einer näheren Betrachtung.

II. Die Entscheidung des Gerichts

Das OVG Münster hatte über einen Antrag auf einstweilige Anordnung zu entscheiden. In einem solchen Eilverfahren schätzt das Gericht dabei in kurzer Zeit - meist innerhalb weniger Tage oder Wochen - die Erfolgsaussichten des Hauptsacheverfahrens, also der regulären Klage, ein. Dann wägt das Gericht auf Grundlage dieser Einschätzung ab, durch welche vorläufige Regelung die beteiligten Interessen am besten sichergestellt werden.[4]

---

1 Zum Hintergrund: https://www.swr.de/kultur/literatur/stadtbibliothek-muenster-wie-neutral-darf-eine-bibliothek-sein-100.html (alle Links des Beitrags wurden zuletzt am 03.12.2025 abgerufen).

2 VG Münster, Beschl. v. 11.04.2025 – 1 L 59/25, GRUR-RS 2025, 7235.

3 OVG Münster, Beschl. v. 08.07.2025 – 5 B 451/25, NJW 2025, 2716.

4 Vgl. § 123 Abs. 1 S. 2 VwGO.

Im Ergebnis hat das OVG Münster dem Autor einstweilen Recht gegeben. Das Gericht verpflichtete die Stadtbibliothek also dazu, die Warnhinweise zu entfernen. Diese Entscheidung gilt zunächst bis zu einer Entscheidung im regulären Klageverfahren. Unklar ist aber derzeit noch, ob die Bibliothek das Hauptsacheverfahren weiter betreiben wird. Das Gericht setzte sich in den Entscheidungsgründen intensiv mit Funktion und Auftrag der öffentlichen Bibliothek auseinander.

1. Warnhinweis als rechtswidriger Zustand?

Der Autor kann sich für sein Begehren, die Warnhinweise entfernen zu lassen, auf einen öffentlich-rechtlichen Folgenbeseitigungsanspruch stützen. Dieser Anspruch ist gesetzlich nicht festgeschrieben, wird aber seit langer Zeit in der Rechtsprechung anerkannt. Er greift immer dann, wenn durch hoheitliches Handeln ein rechtswidriger Zustand geschaffen wurde, der in ein subjektiv-öffentliches Recht eingreift und noch andauert. Liegen all diese Voraussetzungen vor, kann die betroffene Person von der hoheitlichen Stelle die Beseitigung des rechtswidrigen Zustands verlangen.

Die öffentliche Stadtbibliothek Münster ist eine hoheitliche Stelle, die hier mit Wirkung gegenüber dem Autor gehandelt hat, indem sie sein Werk mit einem Hinweis versah. Wesentlicher Streitpunkt im Verfahren war, ob die Bibliothek dadurch auch in rechtswidriger Weise in die subjektiven Rechte des Autors eingegriffen hat.

2. Verletzung der Meinungsfreiheit

Das OVG Münster prüft zur Klärung dieser Frage, ob die Bibliothek durch ihren Warnhinweis den Schriftsteller in seiner Meinungsfreiheit nach Art. 5 Abs. 1 S. 1 Grundgesetz (GG) verletzt hat. Nach Ansicht des Gerichts ist dies der Fall.

Die Meinungsfreiheit hat in der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) einen besonderen Platz. Gemeinsam mit den anderen Kommunikationsfreiheiten ist die Meinungsfreiheit „schlechthin konstituierend“ für unsere freiheitlich-demokratische Staatsordnung.[5] Insbesondere hängt die Demokratie wesentlich daran, dass sich Menschen frei austauschen und ihre Meinung bilden können. Die Meinungsfreiheit schützt daher das Recht, die eigene Meinung in Wort, Schrift und Bild frei zu verbreiten. Dieser Schutz gilt unabhängig davon, ob die Äußerung rational oder emotional, begründet oder grundlos ist.[6] Allein bewusst oder erwiesen unwahre Tatsachenbehauptungen werden nicht vom Schutzbereich erfasst.[7]

Die im Buch niedergeschriebenen Meinungsäußerungen des Schriftstellers fallen also größtenteils in den Schutzbereich der Meinungsfreiheit - ohne Rücksicht auf ihre Qualität. Zwar ist das Bestreiten erwiesener historischer Tatsachen vom Schutzbereich der Meinungsfreiheit nicht umfasst. Da jedoch der Hinweis das gesamte Buch und damit alle dort enthaltenen Äußerungen erfasst, ist die Meinungsfreiheit des Autors unzweifelhaft betroffen.

Das OVG Münster stellt fest, dass die Bibliothek durch ihren Warnhinweis „mittelbar-faktisch“ in die Meinungsfreiheit des Autors eingegriffen hat.[8] Zwar verhindert die Bibliothek mit ihrem Hinweis nicht die Äußerung oder Verbreitung der Meinung. Daher liegt kein unmittelbarer Eingriff vor. Doch der Hinweis führt nach Ansicht des Gerichts dazu, dass die kundgetane Meinung negativ konnotiert wird – insbesondere im Kontrast zu den übrigen 350.000 Werken, die ohne einen entsprechenden Warnhinweis zur Verfügung gestellt werden. In einem aus Sicht des Gerichts vergleichbaren Fall hatte auch der Europäische Gerichtshof für Menschenrechte (EGMR) eine Verletzung der Meinungsfreiheit (Art. 10 Europäische Menschenrechtskonvention) erkannt.[9]

Neben der Meinungsfreiheit sind nach Einschätzung des Gerichts auch weitere Grundrechte des Autors betroffen: Die Pressefreiheit (Art. 5 Abs. 1 S. 2 GG) sowie das Allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG).

---

5 So schon BVerfG, Urteil vom 15.01.1958 - 1 BvR 400/57, NJW 1958, 257, 258.

6 OVG Münster (Fn. 2), Rn. 6.

7 BVerfG, Beschl. v. 10.11.1998 - 1 BvR 1531–96, NJW 1999, 1322, 1324.

8 OVG Münster (Fn. 2), Rn. 9.

9 EGMR, Urteil vom 23.1.2023 – 61435/19, NJW 2024, 739 - Macaté/Litauen.

3. Rechtfertigung durch öffentlichen Auftrag der Bibliothek

Nachdem das OVG Münster den Warnhinweis als Grundrechtseingriff qualifiziert hat, nimmt es die Funktion und Aufgabe der öffentlichen Stadtbibliothek in den Blick. Dabei ist es im bundesweiten Vergleich eine Besonderheit, dass in Nordrhein-Westfalen sogar gesetzliche Regelungen zu den öffentlichen Bibliotheken existieren. In vielen Bundesländern existieren lediglich Benutzungsordnungen.[10] §§ 47, 48 des Kulturgesetzbuchs Nordrhein-Westfalen (KulturGB NRW) enthalten Bestimmungen zu Aufgabe und Funktion der öffentlichen Bibliotheken. Hieraus könnte die Bibliothek unter Umständen zu einem solchen Warnhinweis berechtigt sein.

Die Aufgabe der öffentlichen Bibliotheken besteht darin, einen selbstbestimmten, niedrigschwelligen und ungehinderten Zugang zu Informationen zu bieten.[11] Unter dieser Maßgabe genießen die Bibliotheken die Freiheit, ihr Angebot eigenständig zu kuratieren: „Öffentliche Bibliotheken leisten durch ein fachlich kuratiertes Informationsangebot einen wichtigen Beitrag zur Sicherung der Informationsfreiheit. Daher sind sie bei der Auswahl ihrer Medien unabhängig und an Weisungen nicht gebunden.“ (§ 48 Abs. 4 KulturGB NRW)

Das OVG Münster prüft, ob in dieser gesetzlichen Aufgabenzuweisung die Kompetenz enthalten sein könnte, Bücher mit umstrittenen Inhalten mit entsprechenden Warnhinweisen zu versehen. Im Ergebnis verneint das Gericht dies. Die Aufgabe der Bibliothek liege gerade darin, einen ungehinderten und selbstbestimmten Zugang zu Informationen zu ermöglichen. Ein negativ wertender Hinweis an einem Werk laufe dieser Aufgabe zuwider.

Auch eine Kuratierung im Sinne des § 48 Abs. 4 KulturGB NRW liegt nach Ansicht des Gerichts nicht vor.[12] Die Freiheit der Bibliothek erstrecke sich insbesondere auf die Auswahl und wohl auch auf die Sortierung der Werke - es gehe aber über eine bloße Kuratierung hinaus, inhaltlich abwertende Warnhinweise anzubringen. Das Gericht macht dabei explizit deutlich: Die Entscheidung, das Werk aus sachlichen und fachlichen Erwägungen erst gar nicht in den Katalog aufzunehmen, wäre von der Aufgabenzuweisung gedeckt gewesen.

Insgesamt fehlt es nach Ansicht des OVG Münster daher an einer gesetzlichen Grundlage, die die Grundrechtseingriffe hätte rechtfertigen können. So entschied es im Eilverfahren nach summarischer Prüfung zugunsten des Schriftstellers und gab dessen Antrag statt.

III. Kritik an der Entscheidung

Der Beschluss des OVG Münster hat in der Rechtswissenschaft für einige Aufmerksamkeit gesorgt.

1. Hinweis als Grundrechtseingriff

Zum einen findet sich dogmatische Kritik am Vorgehen des OVG Münster. So wird argumentiert, dass das Gericht zu leichtfertig einen Grundrechtseingriff angenommen habe.[13] Ein Eingriff setze nämlich voraus, dass das staatliche Handeln konkrete Rechtsfolgen nach sich ziehe – diese seien bei dem vorliegenden Warnhinweis aber nicht auszumachen. Zudem wird infrage gestellt, ob der Hinweis überhaupt eine negative Konnotation beinhalte – jedenfalls habe das Gericht dies nicht ausreichend gewürdigt und empirisch belegt.[14] Zugleich räumt die Kritik aber auch ein, dass an derartige Empirie in Gerichtsverfahren keine übersteigerten Anforderungen gestellt werden sollten.

Diese Argumentation lässt jedoch die höchstrichterliche Rechtsprechung zum staatlichen Informationshandeln außer Acht.[15] Es ist anerkannt, dass auch staatliche Informationen einen Eingriff

10 So ist es etwa der Fall in Berlin und Bayern.

11 §§ 47 Abs. 2, 48 Abs. 5 S. 2 KulturGB NRW.

12 OVG Münster (Fn. 2), Rn. 18f.

13 Hilbert, NJW 2025, 2718, 2718.

14 Hilbert, NJW 2025, 2718, 2718.

15 Siehe insbesondere BVerfG, Beschl. v. 17.08.2010 - 1 BvR 2585/06, BeckRS 2010, 53160; BVerwG, Urt. v. 15. 12. 2005 - 7 C 20/04, NJW 2006, 1303; siehe auch BVerfG, Beschl. v. 26.06.2002 - 1 BvR 558/91, NJW 2002, 2621.

darstellen können und die nachteiligen rechtlichen Wirkungen nicht notwendigerweise unmittelbar aus dem staatlichen Handeln resultieren müssen. Ob dies im konkreten Fall erfüllt ist, wäre in der Hauptsache näher zu prüfen – ein Eingriff scheint jedoch keinesfalls von vornherein ausgeschlossen.

Andere Einschätzungen aus der Wissenschaft greifen die Rechtsprechung zum staatlichen Informationshandeln daher auch explizit auf. Diese Stimmen bemerken, dass das OVG Münster die höchstrichterliche Rechtsprechung zwar in Teilen verkennt, aber im Ergebnis überzeugend begründet, dass die Normen des KulturGB NRW den Warnhinweis nicht rechtfertigen können.[16]

2. Hinweis als milderes Mittel?

Ein weiterer Kritikpunkt aus der Literatur verweist auf die Freiheit zur Kuratierung. So habe eine öffentliche Bibliothek unter Beachtung von Sach- und Fachlichkeit sogar die Freiheit, ein Werk erst gar nicht zu berücksichtigen oder aus der Sammlung zu entfernen bzw. zu archivieren. Hierauf weist auch das OVG Münster in seiner Entscheidung explizit hin. Es sei jedoch, so die Kritik, wertungswidersprüchlich, das mildere Mittel eines Hinweises für unzulässig zu halten, während Maßnahmen wie die Nichtberücksichtigung oder Entfernung von der Kuratierungsfreiheit der Bibliothek gedeckt seien.[17]

Dem kann entgegengehalten werden, dass ein inhaltlich negativer, distanzierender Hinweis nicht zwangsläufig ein milderes Mittel, sondern eher ein aliud darstellt. Während die Entfernung die Zugänglichkeit beschränkt, kann der Hinweis zu einer anderen, vorgeprägten Wahrnehmung des Werkes führen. Es dürfte von Autor zu Autor unterschiedlich sein, welche Maßnahme als milder angesehen wird. Die abwertende Stellungnahme einer öffentlichen Bibliothek zum eigenen Werk dürfte für viele Autoren womöglich sogar schwerer wiegen, als in einer einzelnen Sammlung nicht vertreten zu sein.

3. Entscheidung des BVerfG zur Bundeszentrale für politische Bildung

Zuletzt wird kritisiert, dass das OVG Münster die Rechtsprechung des BVerfG[18] zu einem Verfahren gegen die Bundeszentrale für politische Bildung außer Acht ließ.[19] Auch dort positionierte sich die Bundeszentrale als hoheitliche Stelle kritisch gegenüber einer Meinungsäußerung eines Bürgers. Das BVerfG hält derartige Positionierungen nicht für grundsätzlich unzulässig – sie müssten aber „Ausgewogenheit und rechtsstaatliche Distanz“ wahren.[20] Mit diesen Voraussetzungen, wegen derer das VG Münster den Hinweis noch für zulässig hielt, setzte sich das Gericht in der Tat nicht auseinander.
Tatsächlich dürfte der hier streitige Hinweis den Anforderungen aus dem BVerfG-Urteil sogar gerecht werden. Doch dies hilft nicht darüber hinweg, dass es einer rechtfertigenden gesetzlichen Grundlage für den Hinweis bedarf. Insofern könnte sich das OVG Münster auf den Standpunkt stellen, dass es auf die Voraussetzungen des BVerfG im entschiedenen Fall gar nicht ankam.

4. Zwischenergebnis

Es zeigt sich an den Reaktionen aus der Wissenschaft, wie viel Diskussionsstoff der Sachverhalt und die Entscheidung des Gerichts bereithalten. Im Ergebnis scheint das OVG Münster aber eine Entscheidung getroffen zu haben, die in Einklang mit der höchstrichterlichen Rechtsprechung steht.

IV. Bedeutung für wissenschaftliche Bibliotheken

Der Beschluss hat erhebliche Relevanz für Bibliotheken der Hochschulen und Forschungseinrichtungen, bei denen es sich im Regelfall um öffentliche Bibliotheken handelt. Auch sie sollten daher die Rechtsprechung des OVG Münster und gegebenenfalls folgende höchstrichterliche Entscheidungen für den Betrieb ihrer Einrichtungen zur Kenntnis nehmen.

16 Insbesondere Kalscheuer, NVwZ 2025, 1362, 1362f.; ähnliche Stβrichtung auch Muckel, JA 2025, 877, 880.

17 Hilbert, NJW 2025, 2718, 2718f.; so auch Issa, GRUR-Prax 2025, 632.

18 BVerfG, Beschl. v. 17.08.2010 - 1 BvR 2585/06, BeckRS 2010, 53160.

19 Issa, GRUR-Prax 2025, 632.

20 BVerfG, Beschl. v. 17.08.2010 - 1 BvR 2585/06, BeckRS 2010, 53160.

Die Freiheit zur Auswahl der Werke ist für wissenschaftliche Bibliotheken, jedenfalls soweit entsprechendes Landesrecht dies vorgibt, etwas stärker zweckgebunden. In § 50 Abs. 2 S. 1 KulturGB NRW heißt es etwa: „Die [wissenschaftlichen] Bibliotheken gemäß Absatz 1 stellen die für Lehre, Forschung, Studium und Kunstausübung an ihrer Einrichtung erforderlichen Bücher, Zeitschriften und anderen Medienwerke bereit."

Gegebenenfalls müssten demnach auch umstrittene Werke in die Sammlung aufgenommen werden, die aus fachlichen Gründen keinen Mehrwert für die Information der Bevölkerung hätten. Mit inhaltlichen Hinweisen sollten öffentliche Bibliotheken jedenfalls insgesamt vorsichtig umgehen, solange nicht der Gesetzgeber konkrete Befugnisse dafür etabliert.[21]

21 Auch eine solche gesetzliche Befugnis würde zudem verfassungsrechtlich auf dünnen Füßen stehen.

Gefährlich flexibel?

Der risikobasierte Ansatz als Leitmodell europäischer Digitalregulierung zwischen Innovation und Compliance-Chaos

Von Ole-Christian Tech, Münster

Nicht erst seit der immer lauter geführten Debatte um die Reform der Datenschutz-Grundverordnung (DSGVO) wird immer wieder auf den „risikobasierten Ansatz“ verwiesen. Das Konzept der risikobasierten Regulierung ist zu einem der häufigsten Buzzwords des europäischen Daten- und Technologierechts geworden. Aber was genau verbirgt sich eigentlich hinter dem Begriff und welche Anforderungen erwachsen hieraus für die Regelungsadressaten?

I. Der Ursprung des risikobasierten Ansatzes als Regulierungsprinzip

Der risikobasierte Ansatz oder auch risk-based approach ist ein Regulierungsansatz, der ursprünglich aus dem Umweltrecht stammt.[1] Er hat die Funktion, komplexe und mit Unsicherheit behaftete Sachverhalte, die sowohl gesellschaftliche Gefahren als auch Potenziale bergen, zu regulieren. Statt eine risikobehaftete Tätigkeit zu verbieten, erlegt ein risikobasierter Ansatz Akteuren spezifische Schutzpflichten auf, die dem jeweiligen Risiko der konkreten Tätigkeit entsprechen. Beispiele aus dem deutschen Verwaltungsrecht sind das Atomgesetz, das Arzneimittelgesetz oder das Geldwäschegesetz.[2]

Der Begriff des Risikos wird dabei allgemein definiert als der Erwartungswert aus der Eintrittswahrscheinlichkeit eines schädigenden Ereignisses, multipliziert mit der antizipierten Schadenshöhe.[3]

II. Risikobasierter Ansatz im europäischen Digitalrecht

Komplexe und mit Unsicherheit behaftete Sachverhalte finden sich auch und gerade in digitalen Ökosystemen. Die Daten innewohnenden ökonomischen Eigenschaften der Nicht-Rivalität und Polyvalenz sorgen dafür, dass sie für zahlreiche ex ante nicht absehbare Zwecke von verschiedenen Akteuren gleichzeitig genutzt werden können. Gerade dies macht sie so wertvoll und erkenntnisreich für die Wirtschaft und die Wissenschaft. Durch ihre Aggregation, Verknüpfung und Auswertung entstehen neue Nutzungspotenziale, aber auch Risiken für die Betroffenen.

Ähnliche Komplexität bergen auch die Dynamiken von Algorithmen, welche die Phänomene wie Hassrede und Desinformation in sozialen Netzwerken oder die systemische Opazität von KI-Anwendungen (Stichwort: Black-Box-Problematik) bedingen.[4] All diese Phänomene und Technologien werden in der Europäischen Union in den letzten Jahren zunehmend reguliert. Bei aller Kritik an den divergierenden und teils widersprüchlichen Legislativakten zeigt sich jedoch eine Gemeinsamkeit in allen Rechtsakten immer wieder: ein risikobasierter Ansatz.

---

1 Roth-Isigkeit in: Ludwigs, EU-WirtschaftsR-HdB § 41 Rn. 173.

2 Roth-Isigkeit, MMR 2024, 621 (624) m.w.N.

3 Grundlegend hierzu Di Fabio, Risikoentscheidungen im Rechtstaat, S. 74; abstrakt findet sich diese Definition bereits in Art. 24 Abs. 1 DSGVO, wonach der Verantwortliche die „Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen“ ermitteln muss; eine konkrete Legaldefinition findet sich etwa in Art. 2 Abs. 2 lit. q EHDS-VO.

4 Vgl. insgesamt Roth-Isigkeit, MMR 2024, 621 (625).

1. DSGVO

Die DSGVO verfolgt nach eigenem Anspruch einen risikobasierten Ansatz. Dieser soll dazu führen, dass der Zielkonflikt zwischen den Schutzinteressen aufseiten des Betroffenen und den Verarbeitungsinteressen aufseiten des Verantwortlichen dahingehend aufgelöst wird, dass eine Einzelfallbewertung widerstreitender Rechte und Interessen erfolgt. Das datenschutzrechtliche Instrumentarium soll nur in Abhängigkeit von der Gefahr angewendet werden, die von der Datenverarbeitung im Einzelfall für den Betroffenen ausgeht.

Dieser Grundsatz kommt besonders deutlich in Art. 24 Abs. 1 DSGVO zum Vorschein.[5] Dieser verlangt vom Verantwortlichen, „unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen [umzusetzen]." Mit anderen Worten muss der Verantwortliche also eine Risikobewertung seiner Verarbeitungstätigkeiten vornehmen und dem Risiko entsprechende Maßnahmen zum Schutz des Betroffenen ergreifen. Ähnliche Ausprägungen finden sich in Art. 5 Abs. 1 lit. f DSGVO („geeignete technische oder organisatorische Maßnahmen"), Art. 32 DSGVO („dem Risiko angemessenes Schutzniveau" statt absoluter Sicherheit[6]) oder Art. 46 DSGVO („geeignete Garantien").

2. KI-VO

Die Verordnung über künstliche Intelligenz (KI-VO) trägt den risikobasierten Ansatz bisher am deutlichsten. Sie unterscheidet KI-Systeme anhand von vier Risikoklassen:[7]

i. KI-Systeme mit inakzeptablem Risiko (verbotene Praktiken)

Für bestimmte KI-Systeme nimmt der Gesetzgeber typisierend ein untragbares Risiko an und verbietet diese daher vollständig. Dies betrifft nach Art. 5 KI-VO insbesondere den Einsatz bestimmter Systeme wie Social Scoring, kognitive Verhaltensmanipulation oder die biometrische Fernidentifizierung für Strafverfolgungszwecke.

ii. Hochrisiko-KI-Systeme

Diese Systeme haben nach der Systematik des Art. 6 KI-VO in Verbindung mit Anhang III zur KI-VO insbesondere dann ein hohes Risiko, wenn sie in bestimmten kritischen Sektoren Anwendung finden.[8] Beispiele hierfür sind KI-Sicherheitskomponenten in kritischen Infrastrukturen, KI-Anwendungsfälle in der Strafverfolgung, im Migrations-, Asyl- und Grenzkontrollmanagement oder in der Rechtspflege.

Sie werden über ihren gesamten Lebenszyklus von regulatorischen Anforderungen begleitet, etwa einem Risikomanagementkonzept nach Art. 9 KI-VO, Anforderungen an die Data Governance nach Art. 10 oder umfassenden Pflichten zur technischen Dokumentation, Protokollierung und Transparenz nach Art. 11-13 KI-VO. Zudem stellt der Gesetzgeber weitere Anforderungen an die Robustheit, Genauigkeit und IT-Sicherheit der Systeme, vgl. Art. 15 KI-VO.[9]

iii. Systeme mit begrenztem Risiko

Diese Kategorie umfasst Systeme, deren Risiko zwar Transparenzpflichten rechtfertigt, jedoch keine umfassenden Anforderungen wie in Art. 9-13 KI-VO. Zu unterscheiden ist dabei zwischen Systemen mit spezifischem Risiko (Art. 50 KI-VO) und KI-Modellen mit allgemeinem Verwendungszweck (sogenannte General-Purpose AI (GPAI), Art. 51 KI-VO).

Beispiele für diese spezifischen Systeme sind etwa Modelle zur Emotionserkennung, zur Generierung von Deep Fakes oder andere generative Modelle, die ein spezifisches Verwechslungsrisiko

5 Jungkind/Koch, ZD 2022, 656 (657f).

6 Vgl. auch Erwägungsgrund 83 zur DSGVO.

7 Für eine grafische Darstellung dieser abgestuften Risikopyramide siehe auch https://ec.europa.eu/information_society/newsroom/image/document/2021-17/pyramid_7F5843E5-9386-8052-931F5C4E98C6E5F2_75757.jpg (alle Links des Beitrags wurden zuletzt am 19.12.2025 abgerufen).

8 Roth-Isigkeit, MMR 2024, 621 (623).

9 Roth-Isigkeit, MMR 2024, 621 (623).

aufweisen und daher Gegenstand besonderer Offenlegungsverpflichtungen sind.[10]

Eine Besonderheit stellen hier im Rahmen der GPAI-Modelle diejenigen dar, die systemische Risiken bergen, vgl. Art. 51 Abs. 1 KI-VO.[11] Dies ist insbesondere dann der Fall, wenn sie „über Fähigkeiten mit hohem Wirkungsgrad“ verfügen, vgl. Art. 51 Abs. 1 lit. a KI-VO.[12] Anbieter solcher Systeme sind zusätzlich verpflichtet, ihre Modelle nach dem Stand der Technik zu prüfen, standardisierte Modellbewertungen und Angriffstests durchzuführen, um systemische Risiken zu erkennen und zu mindern sowie auftretende Risiken und schwerwiegende Vorfälle zu dokumentieren, vgl. Art. 55 Abs. 1 KI-VO.

iv. KI-Modelle mit minimalem Risiko

Schließlich verbleiben noch KI-Modelle ohne oder mit nur geringem Risiko. Nach Auffassung der Europäischen Kommission fallen hierunter die meisten derzeit verwendeten Systeme. Praktische Beispiele sind etwa KI-Systeme in Videospielen oder Spamfiltern.[13] Sie sind von jeglicher Regulierung durch die KI-VO ausgenommen.

Trotz der stark unterschiedlichen Regelungsintensität der einzelnen Risikostufen zeigt sich ein zentrales Element des risikobasierten Ansatzes: die regulierte Selbstregulierung. Unter einer abstrakten legislativen Risikobestimmung wird eine konkrete Risikobewertung durch die Anbieter selbst vorgeschrieben. Der Verantwortliche ist gehalten, das Verarbeitungsrisiko selbst zu bestimmen und dementsprechend daran anknüpfende Maßnahmen vorzunehmen.

Dieser Ansatz ermöglicht einen Ausgleich zwischen dem Schutz vor negativen Folgen der Technologie und den Innovationschancen.

3. DSA

Auch der Digital Services Act (DSA) folgt einem risikobasierten Ansatz.[14] Die typisierende Annahme des Gesetzgebers ist dabei, dass, je größer eine Online-Plattform ist, desto größer ist auch ihr Einfluss und somit auch das Risiko, das sie für Individuen und die Gesellschaft darstellt. Sehr große Online-Plattformen (Very Large Online Platforms, VLOPs) müssen somit strengere Sorgfalts-, Transparenz- und Berichtspflichten erfüllen als kleinere Plattformen. Damit folgt der DSA, ähnlich wie die KI-VO, einem abgestuften „pyramidalen“ Regulierungskonzept.

Die größenbedingten systemischen Risiken, die der DSA in den Blick nimmt, sind dabei zum Beispiel die Verbreitung rechtswidriger Inhalte, die nachteilige Auswirkungen auf die gesellschaftliche Debatte, auf Wahlprozesse oder die öffentliche Sicherheit sowie nachteilige Auswirkungen in Bezug auf geschlechtsspezifische Gewalt, den Schutz der öffentlichen Gesundheit und von Minderjährigen, vgl. Art. 34 Abs. 1 DSA haben können. Diese Risiken werden naturgemäß durch sogenannte virale Effekte in Empfehlungssystemen verstärkt, die wiederum von der Größe der Plattform abhängen.

Auch hier setzt der Gesetzgeber auf das Instrument der Selbstregulierung: Den VLOPs bzw. VLOSEs wird selbst die Pflicht zur Risikobewertung auferlegt. Art. 35 DSA knüpft an diese Bewertung dann die Pflicht zur Ergreifung angemessener, verhältnismäßiger und wirksamer Risikominderungsmaßnahmen.[15]

Der risikobasierte Ansatz ist also – trotz seiner Prominenz in der datenschutzrechtlichen Debatte – kein isoliertes DSGVO-Konzept, sondern entwickelt sich derzeit immer mehr zum Strukturprinzip des europäischen Digitalrechts.

---

10 Roth-Isigkeit, MMR 2024, 621 (623).

11 Siehe auch Erwägungsgrund 110 zur KI-VO.

12 Siehe auch Erwägungsgrund 111 zur KI-VO.

13 https://digital-strategy.ec.europa.eu/de/policies/regulatory-framework-ai#ecl-inpage-a-risk-based-approach.

14 Roth-Isigkeit, MMR 2024, 621 (624); Siehe auch Efroni, The Digital Services Act: risk-based regulation of online platforms, https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606.

15 Roth-Isigkeit, MMR 2024, 621 (624).

III. Praktische Auswirkungen für Wissenschaft und Forschung

Der Vorteil des risikobasierten Ansatzes besteht darin, dass er technologieoffene Regulierung und damit eine erhöhte Flexibilität für Rechtsanwender auf dem Gebiet einer dynamischen Regulierungsmaterie ermöglicht. Insbesondere für Wissenschaft und Forschung schafft dies Gestaltungsspielräume, um auch risikobehaftete Projekte durchführen zu können, solange diese Risiken durch adäquate Sicherungsmaßnahmen adressiert werden.

Auf der Kehrseite birgt diese Flexibilität naturgemäß aber auch einen weniger klaren Rechtsrahmen und somit Unsicherheiten. Die Verlagerung der Risikobewertung auf die regulierten Akteure selbst führt zu einem erhöhten Compliance-Aufwand. Forschungseinrichtungen müssen eigenständig komplexe Risikobewertungen durchführen und unterliegen hierzu umfangreichen Dokumentationspflichten. Der gesamte Prozess der Risikobewertung und -minimierung muss nachvollziehbar dokumentiert werden. Insbesondere bei neuen Technologien stellt sich regelmäßig die Frage, wann ein Risiko untragbar ist und was „angemessene“ Maßnahmen im Rahmen eines Risikomanagements darstellen. Ob der risikobasierte Ansatz daher tatsächlich die notwendigen Innovationsfreiräume schafft oder durch die Verlagerung der Verantwortung und des administrativen Aufwands auf die Forschungseinrichtungen eher zum Hemmnis für sie wird, bleibt abzuwarten.

Was sind Quasi-Anbieter von KI-Systemen?

In bestimmten Fällen gelten Dritte als Anbieter von Hochrisiko-KI-Systemen nach der KI-VO

Von Philipp Schöbel, Berlin

Die Relevanz der Verordnung über Künstliche Intelligenz (KI-VO) für Hochschulen wird im Infobrief regelmäßig betont[1]. Dabei stand oftmals die Rolle von Hochschulen als Betreiber von KI-Systemen im Fokus. Betreiber können aber auch zu „Quasi-Anbietern" nach der KI-VO werden. Art. 25 KI-VO sieht für bestimmte Fälle vor, dass auch Händler, Einführer, Betreiber oder sonstige Dritte als Anbieter eines Hochrisiko-KI-Systems gelten. Dadurch erweitert sich der Pflichtenkreis für diese Akteure deutlich.

I. Anbieter und Betreiber

Die KI-VO[2] kennt eine Reihe verschiedener Adressaten. Dazu gehören etwa Anbieter, Betreiber, Bevollmächtigte, Einführer und Händler. Mit diesen verschiedenen Adressatenkategorien sind entsprechend unterschiedliche Pflichten verbunden. Dies hängt auch damit zusammen, dass die einzelnen Akteure je nach der Position in der Wertschöpfungskette anders auf die Risiken von KI-Systemen und KI-Modellen einwirken können. Für Hochschulen[3] sind die beiden Adressatenkategorien des Anbieters und des Betreibers besonders relevant. Die Unterscheidung ist wichtig, weil den Anbieter die meisten Pflichten[4] der KI-VO treffen.[5] Es ist aber auch möglich, dass eine Person zugleich Anbieter und Betreiber ist.[6]

1. Anbieter von KI-Systemen

Anbieter nach der KI-VO kann eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle sein. Wer ein KI-System oder KI-Modell mit allgemeinem Verwendungszweck[7] entwickelt oder entwickeln lässt, ist Anbieter, wenn er es zudem unter eigenen Namen oder eigener Handelsmarke in den Verkehr bringt oder in Betrieb nimmt. Es ist unerheblich, ob dies entgeltlich oder unentgeltlich geschieht (Art. 3 Nr. 3 KI-VO). Entwickeln bedeutet sowohl das von Grund auf Neuentwickeln als auch das Anpassen (etwa durch Finetuning).[8] Entwickeln lassen bedeutet, dass der Entwicklungsprozess von einem beauftragten Dienstleister übernommen wird.[9] Inverkehrbringen bedeutet die erstmalige Bereitstellung auf dem EU-Markt (Art. 3 Nr. 9 KI-VO). Bereitstellung auf dem Markt ist die entgeltliche oder unentgeltliche Abgabe zum Vertrieb oder zur Verwendung

---

1 So etwa zuletzt: Schöbel, Das Recht auf Erklärung von KI-Entscheidungen – Teil 1, DFN-Infobrief Recht 10/2025, S. 8; KI-Kompetente Hochschulen, DFN-Infobrief Recht 08/2025, S. 7; die Perspektive um neuere Entwicklungen ergänzend, siehe Yang-Jacobi, Endlich eine Lösung für mehr KI in der Wissenschaft?, DFN-Infobrief Recht 1/2026.

2 Zur Übersicht über die KI-VO siehe: Schöbel, AI Act – Licht der Europäischen Union, DFN-Infobrief Recht 12/2024, S. 7 f.

3 Zur Wissenschaftsausnahme im AI Act siehe: Schöbel, Der AI Act und die Wissenschaft, DFN-Infobrief Recht 2/2025, S. 2.

4 Die Anbieterpflichten nach der KI-VO werden in einem kommenden Infobriefbeitrag ausführlich dargestellt.

5 Kirschke-Biller/Füllsack in: BeckOK KI-Recht, 3. Ed. 1.8.2025, KI-VO Art. 3 Rn. 80.

6 Hilgendorf/Härtlein in: HK-KI-VO , KI-VO Art. 3 Rn. 5.

7 Zur Einstufung eines KI-Modells mit allgemeinem Verwendungszweck siehe: Schöbel, KI-Modelle made in Europe?, DFN-Infobrief Recht 4/2025, S. 15.

8 Kirschke-Biller/Füllsack in: BeckOK KI-Recht, 3. Ed. 1.8.2025, KI-VO Art. 3 Rn. 88.

9 Kirschke-Biller/Füllsack in: BeckOK KI-Recht, 3. Ed. 1.8.2025, KI-VO Art. 3 Rn. 89.

auf dem EU-Markt im Rahmen einer Geschäftstätigkeit (Art. 3 Nr. 10 KI-VO). Inbetriebnahme bedeutet die Bereitstellung eines KI-Systems in der EU zum Erstgebrauch direkt an den Betreiber oder zum Eigengebrauch entsprechend seiner Zweckbestimmung (Art. 3 Nr. 11 KI-VO). Dies umfasst auch die rein interne Nutzung eines selbst entwickelten KI-Systems.[10]

2. Betreiber von KI-Systemen

Der Betreiber kann auch als „Verwender" von KI-Systemen beschrieben werden.[11] Betreiber kann (genauso wie Anbieter) eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle sein. Sie muss das KI-System in eigener Verantwortung verwenden. Ausgenommen sind persönliche und nicht berufliche Tätigkeiten (Art. 3 Nr. 4 KI-VO). Verwendung meint einen bewussten Einsatz. So soll keine Verwendung mehr vorliegen, wenn lediglich der Output eines KI-Systems genutzt wird (die Eingabe von Eingabedaten – also etwa „Prompts"– ist im Gegensatz dazu jedoch von der Verwendung erfasst).[12] Damit ist für Hochschulen die Frage der Betreibereigenschaft maßgeblich anhand der Frage nach der „eigenen Verantwortung" zu beantworten. Eigenverantwortlichkeit meint in diesem Kontext „auf eigene Rechnung und auf eigenes Risiko".[13] Eine Eigenverantwortlichkeit kann etwa vorliegen, wenn eine Verantwortung für das richtige Funktionieren des KI-Systems übernommen wird. Weiterhin wäre Eigenverantwortlichkeit anzunehmen, wenn darüber entschieden wird, in welchen betrieblichen Kontexten ein KI-System eingesetzt wird. Auch eine kontinuierliche Überwachung könnte für einen eigenverantwortlichen Einsatz sprechen.[14] Arbeitnehmer:innen, die ein KI-System in persönlicher und sachlicher Abhängigkeit für ihre(n) Arbeitgeber:innen einsetzen, sind keine Betreiber im Sinne der KI-VO.[15]

II. Quasi-Anbieter

In Art 25 KI-VO sind insgesamt fünf verschiedene Varianten geregelt, nach denen Dritte als Anbieter eines KI-Systems gelten. Die ersten drei Varianten regeln Fälle, die sich auf Anbieter von Hochrisiko-KI-Systemen[16] beziehen. Die letzten beiden Varianten regeln Fälle, in denen Hersteller von Produkten, in die ein Hochrisiko-KI-System als Sicherheitsbauteil integriert ist, ebenfalls als Anbieter dieses KI-Systems gelten.

1. Versehen des KI-Systems mit eigenem Namen oder eigener Handelsmarke

Die erste Variante umfasst Fälle, in denen Dritte ein bereits in Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-KI-System mit ihrem Namen oder ihrer Handelsmarke versehen (Art. 25 Abs. 1 lit. a KI-VO). Dies gilt auch dann, wenn die vertraglichen Vereinbarungen zwischen den Parteien eine andere Pflichtenaufteilung vorsehen. Bei physischen Produkten kann der Name etwa außen auf das Produkt gedruckt oder geklebt werden. Bei reinen Softwareprodukten ist dies selbstredend anders. Hier soll es maßgeblich auf die Begleitumstände wie etwa die Ausgestaltung der Benutzeroberfläche ankommen.[17] Ausreichend soll unter Umständen auch schon die Kennzeichnung in der Gebrauchsanweisung des KI-Systems sein.[18]

10 Bomhard in: derselbe/Pieper/Wende, KI-VO, Art. 3 Rn. 103.

11 Bomhard in: derselbe/Pieper/Wende, KI-VO, Art. 3 Rn. 104.

12 Wendehorst in: Martini/dieselbe, KI-VO, Art. 3 Rn. 83.

13 Wendehorst in: Martini/dieselbe, KI-VO, Art. 3 Rn. 84.

14 Dazu insgesamt: Bomhard in: ders./Pieper/Wende, KI-VO, Art. 3 Rn. 109.

15 Wendehorst in: Martini/dieselbe, KI-VO, Art. 3 Rn. 84.

16 Zu Hochrisiko-KI-Systemen im Hochschulsektor siehe: Schöbel, AI Act – Licht der Europäischen Union, DFN-Infobrief Recht 12/2024, S. 12.

17 Vgl. Kirschke-Biller/Füllsack in: BeckOK KI-Recht, 3. Ed. 1.8.2025, KI-VO Art. 3 Rn. 93.

18 Gössl in: Martini/Wendehorst, KI-VO, Art. 25 Rn. 14.

2. Wesentliche Veränderung eines Hochrisiko-KI-Systems

Wird ein Hochrisiko-KI-System nach Inverkehrbringen oder Inbetriebnahme wesentlich verändert, bleibt aber weiterhin ein Hochrisiko-KI-System, gilt die verändernde Person als Anbieter des Hochrisiko-KI-Systems (Art. 25 Abs. 1 lit. b KI-VO).

Der Begriff der wesentlichen Veränderung wird in der KI-VO legaldefiniert.[19] Dies ist eine Veränderung eines KI-Systems nach dessen Inverkehrbringen oder Inbetriebnahme. Diese Veränderung muss nach der vom Anbieter durchgeführten ursprünglichen Konformitätsbewertung nicht vorgesehen oder geplant gewesen sein. Zudem muss durch die Veränderung die Konformität des KI-Systems mit den Anforderungen des Kapitel III Abschnitt 2 KI-VO beeinträchtigt werden. Alternativ genügt es, wenn die Veränderung zu einer Änderung der Zweckbestimmung führt, für die das KI-System ursprünglich bewertet wurde (Art. 3 Nr. 23 KI-VO).

3. Änderung der Zweckbestimmung eines KI-Systems

Die dritte Variante erfasst Fälle, in denen die Zweckbestimmung eines KI-Systems, das kein Hochrisiko-KI-System ist, geändert wird und das KI-System durch diese Änderung zum Hochrisiko-KI-System wird. Auch der Begriff der Zweckbestimmung wird durch die KI-VO legaldefiniert als die Verwendung, für die ein KI-System laut Anbieter bestimmt ist (Art. 3 Nr. 12 KI-VO). Dies schließt auch besondere Umstände und Bedingungen für die Verwendung ein, also etwa die vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation (Art. 3 Nr. 12 KI-VO).

Wird der Zweck eines KI-Systems geändert, müssen die Voraussetzungen des Art. 6 KI-VO geprüft werden. Dort wird geregelt, wann ein KI-System als Hochrisiko-KI-System eingestuft wird. Art. 6 Abs. 1 KI-VO regelt sogenannte produktbezogene KI-Systeme. Danach ist ein KI-System ein Hochrisiko-KI-System, wenn es zwei Voraussetzungen erfüllt. Die erste Bedingung ist, dass das KI-System entweder selbst unter einen der in Anhang I KI-VO aufgeführten Sekundärrechtsakte fällt oder ein Sicherheitsbauteil eines Produkts ist, das unter einen der aufgeführten Sekundärrechtsakte fällt. Die zweite Bedingung ist, dass das KI-System oder das Produkt, dessen Sicherheitsbauteil das KI-System ist, einer Konformitätsbewertung[20] durch Dritte unterliegen muss.

Die Zweckänderung einzelner Mitarbeiter:innen soll grundsätzlich der Arbeitgeber:in nicht zurechenbar sein (sogenannter Mitarbeiterexzess). Dafür sollen die Arbeitgeber:innen jedoch nachweisen können, dass entsprechende technische und organisatorische Maßnahmen ergriffen wurden. Dies kann etwa durch unmissverständliche Weisungen geschehen.[21] Bisher ist die Frage des Mitarbeiterexzesses im Rahmen der KI-VO noch nicht gerichtlich geklärt.

4. Hochrisiko-KI-Systeme als Sicherheitsbauteile

In der KI-VO sind zwei Fälle geregelt, in denen der Hersteller eines Produkts auch Anbieter eines in das Produkt integrierten KI-Systems ist. Dafür muss das Produkt aber unter einen der Rechtsakte fallen, die in Anhang I Abschnitt A KI-VO aufgeführt sind. Das sind etwa Maschinen, Sportboote oder auch Medizinprodukte. Zudem muss das Hochrisiko-KI-System ein Sicherheitsbauteil sein (Art. 25 Abs. 3 KI-VO). Ein Sicherheitsbauteil ist ein Bestandteil eines Produkts oder KI-Systems, das eine Sicherheitsfunktion erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Eigentum gefährdet (Art. 3 Nr. 14 KI-VO). Wird das Hochrisiko-KI-System zusammen mit dem Produkt unter dem Namen oder der Handelsmarke des Produktherstellers in Verkehr gebracht, gilt der Hersteller des Produkts auch als Anbieter des KI-Systems (Art. 25 Abs. 3 lit. a KI-VO). Gleiches gilt, wenn das Produkt bereits in den Verkehr gebracht wurde und das Hochrisiko-KI-System erst danach unter dem Namen oder der Handelsmarke des Produktherstellers in Betrieb genommen wird (Art. 25 Abs. 3 lit. b KI-VO).

19 Art. 3 Nr. 23 KI-VO.

20 Konformitätsbewertung bezeichnet ein Verfahren, um zu überprüfen, ob ein Produkt den rechtlichen Anforderungen genügt. Dies kann je nach Produktart auf unterschiedliche Weise erfolgen.

21 Dazu insgesamt: Bosman in: BeckOK KI-Recht, 3. Ed. 1.8.2025, KI-VO Art. 25 Rn. 80.

III. Rechtsfolgen

Liegt eine der Varianten vor, gilt der Dritte als Anbieter und muss die Anbieterpflichten erfüllen. Dies umfasst etwa, dass der Quasi-Anbieter sicherstellen muss, dass das Hochrisiko-KI-System die Anforderungen der Art. 8 bis 15 KI-VO erfüllt (Art. 16 lit. a KI-VO). Auch muss ein Qualitätsmanagementsystem eingerichtet werden (Art. 16 lit. c iVm Art. 17 KI-VO). Der Quasi-Anbieter muss des Weiteren dafür sorgen, dass das Hochrisiko-KI-System dem betreffenden Konformitätsbewertungsverfahren unterzogen wird (Art. 16 lit. f KI-VO). Zudem muss der Quasi-Anbieter sich und das KI-System vor dem Inverkehrbringen oder der Inbetriebnahme in der dafür eingerichteten EU-Datenbank registrieren (Art. 16 lit. i iVm Art. 49 Abs. 1 KI-VO).[22]

Der Anbieter, der das KI-System ursprünglich in den Verkehr gebracht oder in Betrieb genommen hat, gilt nicht mehr als Anbieter dieses spezifischen KI-Systems (Art. 25 Abs. 2 S. 1 KI-VO). Dieser ursprüngliche Anbieter arbeitet aber eng mit dem neuen Anbieter zusammen. Zudem stellt er die erforderlichen Informationen zur Verfügung. Überdies sorgt er für den vernünftigerweise zu erwartenden technischen Zugang und die sonstige Unterstützung (Art. 25 Abs. 2 S. 2 KI-VO). Eine Ausnahme gilt, wenn der Erstanbieter eindeutig festgelegt hat, dass sein KI-System nicht in ein Hochrisiko-KI-System umgewandelt werden darf. Diese Pflichten greifen in diesem Fall für den ursprünglichen Anbieter nicht.[23]

IV. Relevanz für Hochschulen

Für Hochschulen ist die Rolle des Quasi-Anbieters besonders relevant, da durch einzelne Handlungen der Pflichtenkreis eklatant erweitert werden kann. Die erste und die dritte Variante dürften dabei besonders bedeutsam sein. Wird ein KI-System mit dem Namen einer Hochschule versehen, dann kann die Hochschule als Anbieterin dieses KI-Systems gelten. Die vertraglichen Vereinbarungen zwischen der Hochschule und der Anbieterin des KI-Systems ändern an den öffentlich-rechtlichen Pflichten der KI-VO in diesem Fall nichts (vgl. Art. 25 Abs. 1 lit. a KI-VO). Weiterhin sollte beim Einsatz von KI-Systemen bedacht werden, ob damit eine Zweckänderung eines KI-Systems hin zur Hochrisiko-KI einhergeht. Zudem ist es wichtig, Mitarbeiter:innen, die mit KI-Systemen arbeiten, anzuweisen, diese nur zweckentsprechend zu nutzen.

22 Die Aufzählung ist nicht abschließend.

23 Gössl in: Martini/Wendehorst, KI-VO, Art. 25 Rn. 38.

DFN Infobrief-Recht-Aktuell

• IT-Sicherheitsrecht: Verkündung des Gesetzes zur Umsetzung der NIS-2-Richtlinie

Am 5. Dezember 2025 wurde das Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung verkündet. Damit ist am 6. Dezember 2025 eine umfassende Modernisierung des Cybersicherheitsrechts in Kraft getreten. Die Anforderungen an die Cybersicherheit der Bundesverwaltung sowie bestimmter Unternehmen werden dadurch erhöht.

Hier erhalten Sie den Link zur Presseerklärung: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/251205_NIS-2-Umsetzungsgesetz_in_Kraft.html

• Plattformrecht: EU-Kommission verhängt Geldbuße in Höhe von 120 Mio. Euro gegen X

Die EU-Kommission hat am 5. Dezember 2025 eine Geldbuße in Höhe von 120 Mio. Euro gegen X verhängt. X hatte gegen seine Transparenzverpflichtungen gemäß dem Gesetz über digitale Dienste (Digital Services Act, DSA) verstoßen. Die Verwendung des „blauen Häkchens" für geprüfte Konten durch X täuscht die Nutzer und stellt eine irreführende Gestaltungspraktik dar. Das Werbe-Repository von X erfüllt zudem nicht die Transparenz- und Barrierefreiheitsanforderungen des Gesetzes. Bemängelt wird außerdem, dass X seinen DSA-Verpflichtungen nicht nachkommt, Forschern Zugang zu den öffentlichen Daten der Plattform zu gewähren.

Hier erhalten Sie den Link zur Presseerklärung der EU-Kommission: :
https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934

• Grundrechte: 25 Jahre Charta der Grundrechte der Europäischen Union (GRCh)

Im Jahr 2000 wurde die GRCh proklamiert. Sie wahrt die Grundwerte der Würde, Freiheit, Demokratie, Gleichheit, Rechtsstaatlichkeit und Achtung der Menschenrechte. Die Charta ist der wichtigste Leitfaden der EU für die Sicherstellung der Einhaltung der Grundrechte in allen politischen Bereichen. Zum 25. Jubiläum der Charta wurde der Jahresbericht 2025 veröffentlicht, der alle Maßnahmen zusammenfasst, die seit 2020 zur Stärkung der Grundrechte ergriffen wurden.

Hier erhalten Sie den Link zum Jahresbericht 2025 über die Anwendung der Charta der EU:
https://commission.europa.eu/document/download/48c1a697-3eeb-4b00-b0ca-bebc2e6eb2d6_en?filename=JUST_template_comingsoon_standard.pdf&prefLang=de

• Plattformrecht: Abweisung der Klage von Amazon gegen Einstufung als „sehr große Online-Plattform" durch den Europäischen Gerichtshof (EuGH)

Der EuGH hat die Klage von Amazon gegen den Beschluss der EU-Kommission, mit dem diese die Plattform als „sehr große Online-Plattform" einstufte, mit Urteil vom 19. November 2025 abgewiesen. Anbietern bestimmter Dienste, die als sehr große Online-Plattformen oder sehr große Suchmaschinen eingestuft werden, obliegen nach dem Gesetz über digitale Dienste besondere Verpflichtungen. Amazon war der Ansicht, dass diese Bestimmungen mehrere Grundrechte der GRCh verletzen.

Hier erhalten Sie den Link zur Pressemitteilung: https://curia.europa.eu/jcms/jcms/p1_5243901/de/

Kurzbeitrag: Endlich eine Lösung für mehr KI in der Wissenschaft?

Die EU-Kommission stellt eine europäische Strategie für KI in der Wissenschaft vor

von Anna Maria Yang-Jacobi, Berlin

Die EU legt weiter nach im Bereich KI. Nachdem die Verordnung für Künstliche Intelligenz (KI-VO)[1] aus produktsicherheitsrechtlicher Sicht für die verantwortungsvolle Entwicklung und Nutzung von KI sorgen soll, folgen nun Maßnahmen zur verstärkten Anwendung von KI. So stellte die EU-Kommission Anfang Oktober 2025 zwei neue KI-Strategien vor.[2] Eine dieser Strategien, „KI in der Wissenschaft", ist für Hochschulen und Forschungseinrichtungen von besonderer Bedeutung.[3]

I. Inhalt der Strategie „KI in der Wissenschaft"

Nach der Regulierung von KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck in der KI-VO soll nun die Anwendung von KI in den Vordergrund der europäischen Bestrebungen treten. Mit der Strategie „KI in der Wissenschaft"[4] will die EU-Kommission im weltweiten „KI-Rennen" aufholen. Immerhin kamen bis 2017 noch ein Großteil der wissenschaftlichen Publikationen zur Forschung mithilfe von KI-Anwendungen von Forschenden in der EU. In der Zwischenzeit überholten die USA und China die EU jedoch. Nun plant die EU, technologische Souveränität zu erreichen und die EU zu einer Drehscheibe für KI-gestützte wissenschaftliche Innovationen zu machen. Langfristig soll die EU zu einem KI-Kontinent[5] werden, der die Grenzen des KI-Einsatzes bei gleichzeitiger Achtung und Stärkung der Menschenrechte und demokratischen Werte weiter ausdehnt.

Ein zentraler Startpunkt, um diese Ziele zu erreichen, ist der Einsatz von KI in der wissenschaftlichen Forschung. KI soll in der Wissenschaft verwendet werden, um auch die Forschung und Entwicklung von KI und die Wissenschaft als Ganzes voranzubringen. Für alle Disziplinen gilt, dass KI zu Zeitersparnissen führt und dabei hilft, komplexe wissenschaftliche Probleme anzugehen und schnellere Innovationen zu erzielen. Dies deckt sich mit allgemeinen Erkenntnissen. Laut einer aktuellen Umfrage „Researcher of the Future"[6] des Wissenschaftsverlags Elsevier sieht eine Mehrheit der über 3.200 befragten Forschenden KI als entscheidende Unterstützung in ihrer Forschung an. Beispielsweise können KI-Tools Forschende bei Literaturrecherchen unterstützen, Forschungsarbeiten zusammenfassen, Forschungsdaten analysieren, Förderanträge aufsetzen oder Forschungsberichte verfassen. Zudem könnten auch Laborversuche automatisiert werden.

---

1 Verordnung (EU) 2024/1689.

2 EU-Kommission, Pressemitteilung vom 8.10.2025, https://ec.europa.eu/commission/presscorner/detail/de/ip_25_2299 (alle Links dieses Beitrags wurden zuletzt am 11.11.2025 abgerufen).

3 Die andere Strategie „KI anwenden" will dazu beitragen, dass das Potenzial von KI in bestimmten Wirtschaftszweigen und dem öffentlichen Sektor in Zukunft tatsächlich genutzt wird.

4 COM (2025) 724 final, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52025DC0724.

5 Generell zum Aktionsplan für den KI-Kontinent, 9.4.2025, https://digital-strategy.ec.europa.eu/de/library/ai-continent-action-plan.

6 Researcher of the Future, Confidence in Research report, 2025, https://assets.ctfassets.net/o78em1y1w4i4/137SmnpRSP2mSuhDxtFdls/72a1777e8a72f3c60748956037f76433/Researcher-Of-The-Future.pdf.

1. RAISE

Im Mittelpunkt der EU-Strategie steht ein neues virtuelles europäisches Institut: die Ressource für KI-Wissenschaft in Europa (engl.: Resource for AI Science in Europe), kurz RAISE. Innerhalb von RAISE bündelt und koordiniert die EU Ressourcen für die Entwicklung und Anwendung von KI in der Wissenschaft. Im Rahmen der Vorüberlegungen zu RAISE hat die EU-Kommission zunächst die größten Herausforderungen für die EU im Bereich Forschung und KI erarbeitet. Erstens bestehen die Forschungsanstrengungen und Ressourcen momentan vielfach auf nationaler Ebene, was zu einer Fragmentierung innerhalb der EU führt. Zweitens gibt es bislang erhebliche Schwierigkeiten beim Zugang zu Rechenressourcen und Datensätzen. Als dritte Herausforderung qualifiziert die EU-Kommission den globalen Wettbewerb um Spitzenkräfte in KI und Wissenschaft. Anhand dieser Analyse entwickelte sie die vier Fokuspunkte von RAISE: Exzellenz und Talente, Rechenleistung, Forschungsförderung und Daten. Am Ende sollen sich Forschende innerhalb einer dynamischen Kooperationsgemeinschaft vernetzen und so gemeinsam die neuesten wissenschaftlichen Fragen mithilfe von KI bewältigen. Das vorrangige Ziel bleibt also: Die KI-Spitzenforschung soll gefördert und KI für einen wissenschaftlichen Fortschritt in allen Disziplinen genutzt werden.

2. Pläne der EU

Die „KI in der Wissenschaft"-Strategie sieht bereits konkretere Maßnahmen innerhalb der vier Fokuspunkte vor. Oftmals geht es um eine finanzielle Förderung. Diese erfolgt in der Regel über die bereits vorhandenen Mittel im „Horizont Europa"-Programm[7]. Im Rahmen von Exzellenz und Talente will die EU spezielle Doktorandenprogramme und Exzellenznetzwerke fördern und Talente mit dem „Choose Europe"-Programm[8] anwerben. So soll ein europäisches Netzwerk für Spitzenforschungslabore im Bereich KI entstehen. Forschende stehen KI-Modellen bisher teilweise noch skeptisch gegenüber. Unsichere Faktoren sind die Ethik, die Genauigkeit, die Sicherheit, der Datenschutz und die Transparenz. Außerdem bemängeln sie, dass es nicht genügend Leitlinien für die Anwendung von KI in der Wissenschaft gebe. Innerhalb der „KI in der Wissenschaft"-Strategie sollen somit Ethikkommissionen und „Living Guidelines on the responsible use of gen AI in research" helfen, die Skepsis auszuräumen.

Im Bereich „Rechenleistung" will die EU 600 Millionen Euro investieren und so einen besseren Zugang zu sogenannten KI-Gigafabriken[9] ermöglichen. KI-Gigafabriken sind große KI-Rechen- und Datenspeicherzentren. Innerhalb dieser Zentren können derzeitige KI-Modelle und KI-Modelle der nächsten Generation entwickelt, trainiert und eingesetzt werden. Dafür soll das EuroHPC-Supercomputing-Netzwerk genutzt werden. Außerdem ist auch die Zusammenarbeit mit Partnern aus dem Privatsektor und der Industrie wichtig.

Bezogen auf Daten will die EU die Wissenschaft bei der Ermittlung strategischer Datenlücken unterstützen. Zusätzlich plant die EU, die für KI in der Wissenschaft benötigten Datensätze zu erheben, aufzubereiten und zu integrieren. Dabei hilft die europäische Datenstrategie, die die Datennutzung und -verfügbarkeit erhöhen will. Wichtig sind dafür die Datenräume.[10] Ein bereits bestehender Datenraum für Forschung und Innovation ist zum Beispiel die Europäische Cloud für offene Wissenschaft.[11] Weitere Datenräume in diesem Bereich und auch in anderen Bereichen wie Medien, Gesundheit oder öffentliche Verwaltung liegen bereits vor oder sollen noch folgen. Innerhalb der KI-Fabriken sollen Datenlabore eingerichtet werden, die verschiedene Daten bündeln und zur Verfügung stellen. Interessant ist zudem, dass im Rahmen der Strategie evaluiert werden soll, wie Forschende eine bessere rechtliche Position beim Zugang zu öffentlich

7 https://commission.europa.eu/topics/research-and-innovation/choose-europe_en.

8 Horizont Europa ist ein europäisches Rahmenprogramm für Forschung und Innovation, das von 2021-2027 läuft. Ziele des Programms sind die Förderung wissenschaftlicher und technologischer Exzellenz, Ausbau der europäischen Wettbewerbsfähigkeit und das Schaffen von Arbeitsplätzen in der Wissenschaft und Forschung. Für weitere Informationen, siehe https://www.consilium.europa.eu/de/policies/horizon-europe/ und für Informationen zu Fördermöglichkeiten in Deutschland, siehe https://www.horizont-europa.de.

9 Zu den Gigafabriken siehe https://germany.representation.ec.europa.eu/news/ki-gigafabriken-76-interessenten-wollen-16-eu-landern-kunstliche-intelligenz-investieren-2025-07-01_de.

10 https://digital-strategy.ec.europa.eu/de/policies/data-spaces.

11 https://open-science-cloud.ec.europa.eu/.

finanzierten Forschungsergebnissen sowie zu Publikationen und Daten für wissenschaftliche Zwecke erlangen können.[12]

Zur Forschungsförderung und -finanzierung sollen die jährlichen KI-Investitionen im Horizont Europa-Programm aufgestockt werden. Zusätzlich möchte die EU die Zusammenarbeit mit der Industrie stärken. Auch private Forschung soll eingebunden werden, und europäische KI-Start-Ups sollen besondere Förderung erhalten.

II. Ausblick

Die EU stellte das Pilotprojekt zu RAISE Anfang November 2025 vor. Noch 2025 soll eine erste Koordinierung von RAISE über ein Sekretariat unter „Horizont Europa" erfolgen, und ein wissenschaftlicher Beirat soll berufen werden. Außerdem will die EU in diesem Zeitraum auch damit beginnen, die Doktoranden- und Exzellenznetzwerke zu finanzieren, in die KI-Gigafabriken zu investieren und die Datenlücken mithilfe der Forschenden zu identifizieren. Die Umsetzung der Strategie wird auch mit dem Europäischen Büro für KI koordiniert. Die weiteren Etappen der „KI in der Wissenschaft"-Strategie sollen bis Ende 2027 erfolgen. Anschließend will die EU-Kommission die Umsetzung der Strategie evaluieren.
Der neue Fokus der Anwendung von KI in der Wissenschaft steht im Einklang mit den sich langsam ändernden Prioritäten der EU. So wird die KI-VO rund 1,5 Jahre nach ihrer Verabschiedung bezüglich der Schaffung von besseren Bedingungen für Innovationen teilweise als hinderlich angesehen.[13] Jüngst häuften sich Meldungen, dass die EU-Kommission die Umsetzungsfristen für die KI-VO verlängern und bestimmte Vorschriften für den Mittelstand lockern könnte.[14] Zwar hält die EU weiter an den Bestrebungen fest, dass europäische KI „ethisch, erklärbar, transparent, rechenschaftspflichtig, zuverlässig, sicher, auf den Menschen ausgerichtet und mit Menschenrechten und gesellschaftlichen Werten vereinbar"[15] sein sollte. Nun scheinen jedoch die Entwicklungs- und die wirtschaftliche Perspektive ins Zentrum der Bemühungen zu rücken.

---

12 Siehe zu der Thematik, Yang-Jacobi, Die Kommerzialisierung der Wissenschaft, DFN-Infobrief Recht 10/2025.

13 Svenja Hahn, MdEP, 8.4.2025, https://www.faz.net/pro/digitalwirtschaft/kuenstliche-intelligenz/svenja-hahn-wir-haben-keine-zeit-zu-verlieren-110408350.html.

14 Daniel Leisegang, Ingo Dachwitz, 7.11.2025, https://netzpolitik.org/2025/digitaler-omnibus-eu-kommission-will-datenschutzgrundverordnung-und-ki-regulierung-schleifen/.

15 COM (2025) 724 final, S. 4, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52025DC0724.

Impressum

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: dfn-verein@dfn.de

Texte:

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der Universität Münster und der Humboldt-Universität Berlin.

Universität Münster
Institut für Informations-,
Telekommunikations- und Medienrecht
-Zivilrechtliche Abteilung-
Prof. Dr. Thomas Hoeren
Leonardo Campus 9, 48149 Münster

Tel. (0251) 83-3863, Fax -38601

E-Mail: recht@dfn.de

Humboldt-Universität zu Berlin
Lehrstuhl für Bürgerliches Recht und Recht der Digitalisierung

Prof. Dr. Katharina de la Durantaye, LL. M. (Yale)
Unter den Linden 11, 10117 Berlin

Tel. (030) 838-66754

Podcast der Forschungsstelle Recht im DFN

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: https://anchor.fm/fsr-dfn