„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

# infobrief recht DFN

4 / 2025
April 2025


## Von Papierbergen zur e-Verwaltung?

Die deutsche Verwaltung wird digitalisiert

## Heute schon geNISt?

Die Umsetzung der NIS-2-Richtlinie durch die Bundesregierung lässt weiter auf sich warten

## KI-Modelle made in Europe?

Ein europäisches Forschungs-Konsortium arbeitet derzeit an mehreren Open-Source-Sprachmodellen

## Kurzbeitrag: Ich check das nicht mehr

Faktenchecks und Communitiy-Notes: Über Grenzen und Anforderungen der Content-Moderation auf sehr großen Online-Plattformen

# Von Papierbergen zur e-Verwaltung?

## Die deutsche Verwaltung wird digitalisiert

*Von Anna Maria Yang-Jacobi, Berlin*

Langsam tut sich etwas in Sachen Verwaltungsdigitalisierung. 2013 verabschie-dete der Bundesgesetzgeber erstmals ein sogenanntes E-Government-Gesetz (EGovG)[1]. Zwischenzeitlich traten weitere nationale Gesetze wie das Onlinezugangsgesetz (OZG)[2] und das Registermodernisierungsgesetz (RegModG)[3] in Kraft. Zusätzlich existieren europäische und landesrechtliche Vorgaben zur Digitalisierung der Verwaltungsvorgänge. All diese Regelungen greifen ineinander und sollen zur modernen Verwaltung beitragen. Die Neuerungen betreffen auch Hochschulen und Forschungseinrichtungen.

## I. Die Digitalisierung innerhalb der Behörden

Computer werden in deutschen Behörden bereits seit den 1960er Jahren verwendet.[4] Punktuelle Anpassungen in den Verwaltungsverfahrensgesetzen (VwVfG) und der Verwaltungsgerichtsordnung sowie in bestimmten anderen Gesetzen folgten.[5] 2013 machte der deutsche Gesetzgeber dann einen entscheidenden Schritt in Richtung rechtlich systematischer Verwaltungsdigitalisierung und verabschiedete ein bundesweites EGovG. Ziel des EGovG ist es, die Kommunikation von Bürger:innen mit der Verwaltung auf elektronischem Weg zu vereinfachen. Medienbrüche, also beispielsweise das Ausdrucken eines ursprünglich digitalen Dokuments, um es in der Akte in Papierform abzuheften, sollten der Vergangenheit angehören. Zusätzlich sollte so das Angebot von elektronischen Verwaltungsdiensten einfacher, nutzerfreundlicher und effizienter gestaltet werden.

Das EGovG gilt als Bundesgesetz nach § 1 Abs. 1, Abs. 2 EGovG grundsätzlich nur für die öffentlich-rechtliche Verwaltungstätigkeit der Bundesbehörden und juristischen Personen des öffentlichen Rechts sowie für die Länderverwaltungen, sofern sie Bundesrecht ausführen. Letzteres gilt sowohl für die Ausführung der Länder in eigenen Angelegenheiten zum Beispiel bei der Auszahlung von Wohngeld (Art. 83, 84 Grundgesetz (GG)) als auch bei Auftragsangelegenheiten des Bundes wie bei der Verwaltung der Autobahnen (Art. 85 GG). Um auch landesrechtliche Verwaltungstätigkeiten zu umfassen, existieren in den Bundesländern separate Landesgesetze mit eigenen Bestimmungen zum E-Government in der Landesverwaltung.[6]

Durch die Gesetze werden den Bürger:innen keine zusätzlichen Pflichten auferlegt. Die Regelungen enthalten ausschließlich Verpflichtungen für die Verwaltung. Für die Bürger:innen sollte lediglich eine weitere Möglichkeit entstehen, um mit der Verwaltung zu kommunizieren. So wurden durch das EGovG primär

1 Gesetz zur Förderung der elektronischen Verwaltung vom 25.7.2013, BGBl. I S. 2749.

2 Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen vom 14.8.2017, BGBl. I S. 3122, 3138.

3 Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze vom 28.3.2021, BGBl. I S. 591.

4 Siehe nur Bull, Verwaltung durch Maschinen, 1964.

5 Beispielsweise die Möglichkeit zur Übermittlung elektronischer Dokumente in der Sozialgesetzgebung nach § 36a Sozialgesetzbuch (SGB) I und nach § 87a Abgabenordnung (AO) an Finanzbehörden oder auch der elektronisch Identitätsnachweis nach § 10 PAuswG.

6 Hamburg ist als letztes Bundesland nachgezogen und hat am 19.11.2024 das Hamburgische Verwaltungsdigitalisierungsgesetz verkündet, das am 30.11.2024 in Kraft trat.

die formellen Bestandteile des E-Governments geschaffen bzw. bisherige Hindernisse beseitigt. Die Landesgesetze zum E-Government enthalten ähnliche Regelungen. Allem voran steht die Pflicht der Behörden, einen Zugang zur Übermittlung elektronischer Dokumente zu eröffnen. Weitere Pflichten betreffen die Bereitstellung von Informationen über Behörden online, elektronische Bezahlmöglichkeit/e-Rechnungen, die elektronische Aktenführung und die Optimierung von Verwaltungsabläufen. Außerdem enthalten das EGovG und die Mehrheit der landesrechtlichen E-Government-Gesetze ähnliche Regelungen zu Verwaltungsportalen. Auch die Umsetzung von Standardisierungsbeschlüssen des IT-Planungsrats[7] ist oftmals Teil der gesetzlichen Vorgaben. Bestimmte Regelungen wurden mit den Jahren angepasst oder neu eingefügt wie die §§ 9 lit. b, lit. c EGovG mit Rechtsgrundlagen zur Verarbeitung personenbezogener Daten durch die Behörden, sowie die Bereitstellung von Open Data[8] gemäß § 12a EGovG oder die Nutzung von Open-Source- Programmen nach § 16a EGovG. Eine wichtige Komponente der Verwaltungsdigitalisierung stellt das Once-Only-Prinzip dar. Das Once-Only-Prinzip der Verwaltung zielt auf eine Vereinfachung, indem Bürger:innen oder Unternehmen ihre Daten und Dokumente nur einmal mitteilen müssen. Die öffentliche Verwaltung soll die Nachweise danach über Register abfragen oder mit anderen Behörden austauschen können.[9]

2024 wurde mit § 5 Abs. 1, Abs. 3 EGovG eine allgemeine Vorschrift zur Umsetzung des Once-Only-Prinzips in das EGovG eingefügt. Bei antragsgebundenen Verwaltungsverfahren hat die antragstellende Person nun die Wahl, einen automatisierten Nachweisabruf durch die Behörde zu veranlassen oder den Nachweis selbst digital zu erbringen.

Staatliche Hochschulen und Forschungseinrichtungen sind regelmäßig Körperschaften des öffentlichen Rechts.[10] Als solche gehören sie zur öffentlichen Verwaltung. Im Bereich des E-Governments sind Umstellungen auf elektronische Bewerbungen, elektronische Immatrikulationen oder elektronische Prüfungsanmeldungen denkbar. Da Bildung Sache der Bundesländer ist,[11] richten sich die Bestimmungen nach dem Landesrecht. Sofern die Hochschulen öffentlich-rechtlichen Verwaltungstätigkeiten nachkommen, sind die E-Government-Gesetze der jeweiligen Bundesländer von Bedeutung. Diese handhaben den Geltungsbereich der Regelungen für die elektronische Verwaltung unterschiedlich. In einer Mehrheit der Bundesländer gelten die E-Government-Gesetze bzw. Digitalisierungsgesetze grundsätzlich auch für staatliche Hochschulen. Die Hochschulen müssen je nach Landesrecht beispielsweise sicherstellen, dass ein Zugang für die Übermittlung elektronischer Dokumente eröffnet, digitale Zahlungen ermöglicht oder eine elektronische Akte angelegt werden kann. Teilweise sind die Hochschulen jedoch von bestimmten Pflichten ausgenommen.[12] In manchen Bundesländern gelten zudem spezielle Fristen für die Umsetzung ausgewählter Pflichten.[13]

Die Hochschulen sind in sechs Bundesländern jedoch nicht vom Geltungsbereich der jeweiligen E-Government-Gesetze erfasst.[14] Die Bundesländer begründen dies in der Regel damit, dass Hochschulen weniger Verwaltungstätigkeiten ausführen

7 Ausführlicher zum IT-Planungsrat, Yang-Jacobi, Föderal. Digital. Gut., DFN-Infobrief Recht 2/2025.

8 Offene Daten sind maschinenlesbare Datenbestände, die die Behörden zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben erhoben haben oder durch Dritte haben erheben lassen. Diese sollen z.B. die Bundesbehörden nach § 12a Abs. 1 EGovG zum Datenabruf über öffentlich zugängliche Netze bereitstellen. Personenbezogene Daten sind gem. § 12a Abs. 3a EGovG ausgenommen. Die Verpflichtung ist gerade mit Blick auf den Data Governance Act interessant. Zum DGA siehe: Tech, Datenstaat oder Datensalat?, DFN-Infobrief Recht 8/2023.

9 https://www.digitale-verwaltung.de/SharedDocs/faqs/Webs/DV/DE/servicestandard/nutzerzentrierung-faqs/4-once-only-prinzip.html.

10 Beispielhaft sind §§ 1, 2 Berliner Hochschulgesetz zu nennen.

11 Art. 30, 70 GG.

12 In Hessen gelten gem. § 1 Abs. 2 Nr. 3 HeGovG die Vorschriften zur elektronischen Aktenführung (§ 7 S. 1, S. 2 HeGovG) und zur behördenübergreifenden Zusammenarbeit (§ 14 Abs. 1 HeGovG) nicht für Hochschulen.

13 In NRW soll die elektronische Aktenführung sowie die Abwicklung von Verwaltungsabläufen auf elektronischem Weg bei Hochschulen spätestens ab dem 31.12.2025 erfolgen (§ 9 Abs. 3 S. 4 EGovG NRW, § 12 Abs. 1 S. 1 EGovG NRW; § 14 Abs. 2 S. 1 EGovG NRW stellt eine weitere besondere Frist dar). In Schleswig-Holstein sollte die elektronische Akte bei Hochschulen bis spätestens 31.12.2024 eingeführt sein (§ 4 Abs. 4 EGovG SH).

14 Die Ausnahmen sind Baden-Württemberg (§ 1 Abs. 2 Nr. 3 EGovG BW), Bremen (§ 1 Abs. 3 Nr. 11 BremEVerwG), Niedersachsen (§ 3 Abs. 3 Nr. 1 NDIG), Rheinland-Pfalz (§ 1 Abs. 2 Nr. 6 EGovGRP), Sachsen-Anhalt (§ 1 Abs. 3 S. 1 Nr. 4 EGovG LSA) und Thüringen (§ 1 Abs. 4 S. 1 ThürEGovG). Bis zu einer Änderung mit Wirkung zum 1.1.2023 waren auch in Mecklenburg-Vorpommern Hochschulen vom Geltungsbereich ausgenommen.

und mehr der Lehre und Forschung nachkommen. Lehre und Forschung unterstehen gemäß Art. 5 Abs. 3 GG einem besonderen grundrechtlichen Schutz.[15] Die Hochschulen genießen demnach auch eine gewisse Unabhängigkeit (sogenannte Hochschulautonomie). In diesen Bundesländern müssen die Hochschulen den Pflichten des E-Governments nicht auf Grundlage eines Gesetzes nachkommen. Das bedeutet allerdings nicht, dass die Hochschulen in diesen Bundesländern hinsichtlich der Digitalisierung von Verwaltungsverfahren in Verzug sind. Es gibt auch und gerade dort eigene Initiativen, um die Hochschuldigitalisierung voranzutreiben.[16]

## II. Der digitale Zugang zu Verwaltungsleistungen

Neben dem EGovG gibt es mit dem OZG ein weiteres Bundesgesetz zur Verwaltungsdigitalisierung. Das OZG gilt nach § 1 Abs. 1 OZG für die Verwaltungsleistungen der öffentlichen Stellen von Bund und Ländern, einschließlich der Gemeinden. Landesrechtliche Versionen des Gesetzes sind also nicht möglich. Art. 91c Abs. 5 GG weist dem Bund die Gesetzgebungskompetenz für den übergreifenden informationstechnischen Zugang zu Verwaltungsleistungen von Bund und Ländern zu. Gerade weil das OZG einheitliche Vorgaben für Bund und Länder trifft, stellt es eine treibende Kraft bei der Digitalisierung von Verwaltungsabläufen dar. Bevor die neuesten Veränderungen im OZG durch das Gesetz zur Änderung des Onlinezugangsgesetzes (OZG 2.0)[17] vorgestellt werden, ist ein kurzer Blick auf die grundsätzlichen Regelungen des OZG zu werfen.

### 1. Geschichte des OZG

Das OZG trat im August 2017 in Kraft – kurz nach Einführung des Art. 91c Abs. 5 GG.[18] Durch das Gesetz sollten die vielen Lücken im Online-Angebot von Verwaltungsleistungen geschlossen werden. Davon umfasst sind alle Verwaltungsleistungen, bei denen keine rechtlichen, tatsächlichen oder auch wirtschaftlichen Gründe gegen ein digitales Bereitstellen sprechen. Einen einklagbaren Anspruch auf eine elektronische Zurverfügungstellung der Verwaltungsleistungen hatten Bürger:innen damals allerdings nicht.[19]

Außerdem sieht das OZG vor, dass Verwaltungsleistungen digital über Verwaltungsportale angeboten werden, und die Verwaltungsportale wiederum zu einem Portalverbund zusammengeschlossen werden. Im Portalverbund sollten Nutzerkonten zur einheitlichen Identifizierung für Bürger:innen und Unternehmen bereitstehen. Schon in der Gesetzesfassung von 2017 enthielt das OZG Vorgaben zur elektronischen Abwicklung von Verwaltungsverfahren und Ermächtigungen für nachfolgende Rechtsverordnungen zur IT-Sicherheit und den Kommunikationsstandards zum Austausch zwischen den Verwaltungsportalen sowie eine Rechtsgrundlage zur Verarbeitung personenbezogener Daten. Sanktionsmöglichkeiten sind im OZG nicht vorgesehen.

Für die Umsetzung des OZG war ein Zeitraum von fünf Jahren, also bis Ende 2022, angesetzt. Vor allem Verwaltungsleistungen, die bisher noch nicht online verfügbar waren, sollten bis dahin digital bereitgestellt werden. Die Fristsetzung sollte den Digitalisierungsprozess beschleunigen. In den nachfolgenden Jahren wurde das OZG mehrfach angepasst. Die umfangreichsten Veränderungen folgten mit dem OZG 2.0.

---

15 Normalerweise können sich juristische Personen des öffentlichen Rechts als Teil des Staates nicht auf einen Schutz der Grundrechte berufen. Der Staat kann nicht gleichzeitig Adressat und damit also verpflichtet sein, Grundrechte einzuhalten und Träger und damit berechtigt sein, sich auf die Grundrechte zu berufen (sogenanntes Konfusionsargument). Es gibt jedoch Ausnahmen für juristische Personen des öffentlichen Rechts, wenn sie einem unmittelbar durch bestimmte Grundrechte geschützten Lebensbereich zugeordnet sind. Bei staatlichen Hochschulen ist dies die Wissenschaftsfreiheit nach Art. 5 Abs. 3 S. 1 GG.

16 Diese Entwicklung ist unter anderem auch auf die Pflichten des OZG zurückzuführen (siehe unten). Als Beispiele sind das baden-württembergische Konzept bwUni.digital oder die Uni Göttingen in Niedersachsen zu nennen, Hochschulrektorenkonferenz, Interview mit Dr. Harald Gilch, 6.7.2021, https://www.hrk-modus.de/ressourcen/blog-standpunkte/digitalisierung-an-hochschulen/ (alle Links dieses Beitrags wurden zuletzt am 19.2.2025 abgerufen).

17 BGBl. 2024 I Nr. 245 vom 23.7.2024, Art. 1, https://www.recht.bund.de/bgbl/1/2024/245/VO.

18 Zur Entstehungsgeschichte und Bedeutung von Art. 91c GG: Yang-Jacobi, Föderal. Digital. Gut., DFN-Infobrief Recht 2/2025.

19 BT-Drs. 18/11 135, S. 91, https://dserver.bundestag.de/btd/18/111/1811135.pdf.

## 2. Die Neuerungen des OZG 2.0 und das heutige OZG

Das ursprünglich angestrebte Ziel, 575 Verwaltungsleistungen bis Ende 2022 bundesweit digitalisiert zur Verfügung zu stellen, wurde nicht erreicht. Tatsächlich waren 2022 nur 33 Verwaltungsleistungen flächendeckend über den Portalverbund digital zugänglich.[20] Im Juli 2024 trat – nach langen Verhandlungen – das OZG 2.0 in Kraft. Drei Neuerungen waren von besonderer Bedeutung.

Erstens müssen Bund und Länder Verwaltungsleistungen gemäß § 1a Abs. 1 S. 1 OZG auch elektronisch über Verwaltungsportale anbieten. Um die Nutzung attraktiver zu machen, sollen einige Verwaltungsleistungen auch über eine App angeboten werden.[21] Dies sind noch keine außergewöhnlichen Regelungen. Wirklich neu ist allerdings das Digital-Only-Prinzip in § 1a Abs. 1 S. 2 OZG. Verwaltungsleistungen, die der Ausführung von Bundesgesetzen dienen und ausschließlich Unternehmen als Nutzer betreffen, müssen ab 2030 ausschließlich elektronisch angeboten werden. Davon macht das Gesetz in § 1a Abs. 1 S. 3 OZG eine Ausnahme, indem ein Abweichen vom Digital-Only-Prinzip bei berechtigtem Interesse des Unternehmens möglich ist. Die Einführung des Digital-Only-Prinzips ist bei Verwaltungsleistungen für Unternehmen sinnvoll, da Unternehmen im Vergleich zu Bürger:innen häufiger mit der Verwaltung in Berührung kommen, regelmäßig digitalaffin sind und bereits jetzt Verwaltungsleistungen überwiegend digital in Anspruch nehmen.[22] Nach § 1a Abs. 2 S. 1 OZG haben Nutzer – also auch Bürger:innen – ab 2029 auch einen Anspruch auf einen elektronischen Zugang zu den Verwaltungsleistungen des Bundes. Nach § 1a Abs. 3 OZG soll eine eigene Suchmaschine für den „Katalog“ von Verwaltungsleistungen bereitgestellt gestellt werden. So wird eine staatliche Alternative zu privaten Suchmaschinenanbietern geschaffen.[23]

Zweitens soll der Bund gemäß § 3 Abs. 1 S. 1 OZG ein zentrales Bürgerkonto[24] zur Identifizierung und Authentifizierung von Bürger:innen bereitstellen. Dadurch können die elektronischen Verwaltungsleistungen im Portalverbund in Anspruch genommen werden. Über das Konto soll nach § 2 Abs. 5 S. 1 OZG zusätzlich eine sichere Kommunikation mit der öffentlichen Verwaltung möglich sein. Bei Vorgängen können Bürger:innen direkt nachfragen und Antworten der zuständigen Stelle auf unmittelbarem Weg ins digitale Postfach bekommen. Der Identitätsnachweis muss je nach Vertrauensniveau der elektronischen Verwaltungsleistung über unterschiedliche Verfahren nachgewiesen werden, § 3 Abs. 4 OZG. Die jeweiligen Identifizierungsmittel müssen dabei das Vertrauensniveau der eIDAS-VO[25] erfüllen. Die eIDAS-VO ist eine europäische Verordnung und schafft einen in Europa verbindlichen und einheitlichen Rahmen für eine elektronische Identifizierung und Vertrauensdienste. Vertrauensdienste sind nach Art. 3 Nr. 16 eIDAS-VO Dienste zur Erstellung, Überprüfung und Validierung einer elektronischen Signatur oder auch eines elektronischen Siegels und Zeitstempels, elektronischer Einschreiben und Webseiten-Zertifikate.

Die eIDAS-VO wurde 2024 ebenfalls aktualisiert und enthält mittlerweile Vorschriften zur Einführung einer europäischen digitalen Identität (EUDI). Für das Bürgerkonto kann der Identifikations- und Authentifizierungsnachweis nach § 3 Abs. 4 OZG nun beispielsweise über den Online-Personalausweis (eID) oder dem steuerlichen ELSTER-Zertifikat erfolgen. Ob Bürger:innen ein solches Online-Konto nutzen möchten, bleibt immer noch freiwillig, § 3 Abs. 1 S. 2 OZG. Perspektivisch soll die bisherige

---

20 Kretschmer, Warum der „Behörden-Booster“ klemmt, 29.12.2022, https://www.tagesschau.de/inland/innenpolitik/online-zugangsgesetz-101.html.

21 BT-Drs, 20/8093, S. 35, https://dserver.bundestag.de/btd/20/080/2008093.pdf.

22 BT-Drs, 20/8093, S. 35, https://dserver.bundestag.de/btd/20/080/2008093.pdf.

23 Im Zusammenhang mit europäischen Suchmaschinen ist auch die Entwicklung eines europäischen Suchmaschinenindex zu erwähnen, siehe Yang-Jacobi, Google im Visier der Behörden und Gerichte, DFN-Infobrief Recht 1/2025.

24 Die Unterscheidung von Nutzerkonten in Bürger- und sogenannte Organisationskonten besteht seit Ende 2020. Das Organisationskonto steht Unternehmen und Behörden gem. § 2 Abs. 5 S. 4 OZG zur Verfügung.

25 Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

BundID zur DeutschlandID das zentrale Bürgerkonto werden.[26] Eine Schnittstelle zur EU ID-Wallet[27] ist geplant.

Drittens regelt § 9a Abs. 5, 6 OZG den Ersatz der Schriftform. In Deutschland bedarf es für die Beantragung einiger Verwaltungsleistungen noch der Schriftform. Sofern Nutzende über das Nutzerkonto einen Identitätsnachweis erbracht haben und über ein Verwaltungsportal mittels Online-Formular eine digitale Erklärung abgeben, ersetzt dies nach § 9a Abs. 5 OZG nun die Schriftform. Aus Perspektive der öffentlichen Verwaltung erfolgte ebenso eine Vereinfachung. So kann nach § 9a Abs. 6 OZG ein qualifiziertes elektronisches Siegel der Behörde die Schriftform bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten einer Behörde ersetzen. Ein elektronisches Siegel ist nach Art. 3 Nr. 25 eIDAS-VO auch eine logische Verbindung oder ein Beifügen von elektronischen Daten mit bzw. zu anderen Daten in elektronischer Form. Bescheide können so einfacher übermittelt werden. Bisher fungierte nach dem § 3a Abs. 2 VwVfG nur eine qualifizierte elektronische Signatur als Schriftformersatz. Elektronische Signaturen sind gemäß Art. 3 Nr. 10 eIDAS-VO Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und zum Unterzeichnen verwendet werden. Bislang erlassen Behörden nur selten Bescheide mit qualifizierter elek-tronischer Signatur, da die erlassende Person eine Signaturkarte und einen passenden PIN-Code braucht. Im Gegensatz dazu ist das elektronische Siegel ein personenunabhängiges Organisationszertifikat (Art. 3 Nr. 29 f eIDAS-VO). Somit kann es für juristische Personen oder sonstige Organisationen ausgestellt werden.[28] Die Handhabung ist folglich einfacher. Das elektronische Siegel ist das digitale Gegenstück des Behördenstempels und verringert den administrativen Aufwand.

In Zukunft wird sich zeigen, ob das OZG 2.0 zum erhofften Erfolg der Verwaltungsdigitalisierung führt. Das OZG 2.0 stellt einen Kompromiss von Bund und Ländern dar. Der Bund und die Länder übernehmen die tatsächliche Digitalisierung der Verwaltungsleistungen nach wie vor eigenständig und damit dezentral; die Zuständigkeiten wurden nicht verteilt.[29] Die längeren Fristen bis zur notwendigen Umsetzung beschleunigen den Prozess auch nur bedingt.[30]

## 3. Nationale Ergänzung zum OZG: Die Registermodernisierung

Um zur nutzungsfreundlichen Ausgestaltung des OZG beizutragen, sollte das Once-Only-Prinzip in der Verwaltung möglichst effektiv umgesetzt werden. Der deutsche Gesetzgeber verabschiedete dafür 2021 das Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz; RegMoG). Register sind elektronisch geführte Datenbestände der Verwaltung. Über die Register können Daten und Nachweise zwischen Bürger:innen und der Verwaltung elektronisch übermittelt werden. Für den sicheren elek-tronischen Datenaustausch musste ein registerübergreifendes Kennzeichen zur Identifizierung und Zuordnung festgelegt werden. Mit dem RegMoG entschied sich der Gesetzgeber dafür, die einheitliche Identifikationsnummer nach § 139b AO, die sogenannte Steuer-ID, zu verwenden. So können die Daten von Bürger:innen in einem Verwaltungsverfahren eindeutig zugeordnet werden, und bereits vorhandene Daten der Person müssen nicht erneut nachgewiesen werden. Das Bundesverfassungsgericht stellte allerdings bereits 1983 fest, dass die Einführung eines einheitlichen, für alle Register geltenden Personenkennzeichens ein entscheidender Schritt auf dem Weg zu einer zwangsweisen Registrierung und Katalogisierung der Persönlichkeit und damit ein Verstoß gegen die Menschenwürde nach Art. 1 Abs. 1 GG ist.[31] Gerade in Datenschutzkreisen war (und ist) die einheitliche

26 Wölbert, Wie die BundID zur „DeutschlandID“ werden soll, 12.1.2025, https://www.heise.de/news/Auf-dem-Weg-zur-DeutschlandID-Wie-es-mit-der-BundID-weitergeht-10237147.html.

27 https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/eudiwallet-was-sie-zur-digitalen-brieftasche-wissen-muessen-95821.

28 BT-Drs, 20/8093, S. 25, https://dserver.bundestag.de/btd/20/080/2008093.pdf.

29 Buckler, DöV 2025, 9, 17; Pressemitteilung des Normenkontrollrats, 23.2.2024, https://www.normenkontrollrat.bund.de/Webs/NKR/SharedDocs/Pressemitteilungen/DE/2024/2024-02-23-bundestag-verabschiedet-ozg.html?nn=154834.

30 Guckelberger, DöV 2024, 849, 860.

31 BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, Rn. 110 – Volkszählungsurteil.

Identifikationsnummer umstritten.[32] Das Risiko eines Missbrauchs erhöht sich immerhin, wenn die sensiblen Daten miteinander über verschiedene Register hinweg mit einer Kennziffer verknüpft sind.[33] Als datenschützende Maßnahme führte der Gesetzgeber das Datenschutzcockpit ein.[34] Das Datenschutzcockpit ist gemäß § 10 Abs. 1 S. 1 OZG eine IT-Komponente, mit der sich natürliche Personen, also Bürger:innen, Auskünfte zu Datenübermittlungen zwischen öffentlichen Stellen anzeigen lassen können. So soll ein transparenter Umgang mit den personenbezogenen Daten gewährleistet werden.[35]

Ende 2024 wurde zudem ein weiteres Vorhaben der Verwaltungsdigitalisierung beschlossen. Der Vertrag über die Errichtung und den Betrieb des Nationalen Once-Only-Technical-Systems (NOOTS)[36] ist ein Staatsvertrag zwischen Bund und Ländern nach Art. 91c Abs. 1 GG, Abs. 2 GG. Das NOOTS ist ein gemeinsames flächendeckendes IT-System, das den Datenaustausch zwischen allen öffentlichen Stellen automatisiert. Diese „Datenautobahn" soll künftig eine sichere und effiziente Vernetzung der Verwaltungsdaten ermöglichen, sodass Daten und Nachweise im Einklang mit dem Once-Only-Prinzip nur ein einziges Mal eingegeben werden müssen und bei Bedarf abgerufen werden können. Die Wiederverwendung erfolgt nur bei Zustimmung der Nutzenden.

## 4. Und was macht die EU?

Die EU blieb in Sachen europaweite Verwaltungsdigitalisierung nicht untätig. Das Once-Only-Prinzip (gerade europaweit) ist beispielsweise schon seit 2016 Teil des EU-eGovernment-Aktionsplans.[37] 2018 beschlossen das EU-Parlament und der Europäische Rat zudem die Verordnung zum Single Digital Gateway (SDG-VO).[38] Ziel war es, ein einheitliches digitales Zugangstor zur Verwaltung innerhalb der EU zu schaffen. Der Verwaltungsaufwand für Bürger:innen und Unternehmen sollte reduziert und eine einfachere Teilhabe am Binnenmarkt möglich sein. Dafür sollten Informationen, Verfahren und Unterstützungsdienste in allen Sprachen der EU auf einer zentralen Plattform zugänglich gemacht werden. Das Ziel ist also, parallel zum OZG, das digitale Verwaltungsangebot bürgernah und nutzerfreundlich zu gestalten. Die EU-Mitgliedstaaten waren verpflichtet, bis Ende 2023 ihre Verwaltungsleistungen über das „Your Europe-Portal"[39] elektronisch bereitzustellen und so grenzüberschreitend verfügbar zu machen. Die rechtzeitige Umsetzung gelang den Mitgliedstaaten jedoch nicht.[40] In Deutschland ist das Vorhaben in die OZG-Umsetzung und Registermodernisierung integriert und kein eigenständiges Projekt.

---

32 DSK-Entschließung, Registermodernisierung verfassungskonform umsetzen!, 26.8.2020, https://www.datenschutzkonferenz-online.de/media/en/20200828_entschließung_pkz_final_1.pdf; 32. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit, BT-Drs. 20/10800, S. 99-104, https://dserver.bundestag.de/btd/20/108/2010800.pdf.

33 Ein datenschutzfreundlicheres Domänen-ID-Modell mit mehreren bereichsspezifischen IDs wurde unter anderem aus Kostengründen verworfen, siehe Menhard, Automatisierung auf Kosten der Sicherheit, 11.10.2023, https://netzpolitik.org/2023/registermodernisierung-automatisierung-auf-kosten-der-sicherheit/.

34 v. Lewinski, in: BeckOK DatenschutzR, 50. Edition, Stand: 1.11.2023, DSGVO Art. 87 Rn. 53a.

35 BT-Drs. 19/24226, S. 80, https://dserver.bundestag.de/btd/19/242/1924226.pdf.

36 Vertrag über die Errichtung und den Betrieb des Nationalen Once-Only-Techincal-Systems (NOOTS), https://www.bundesregierung.de/resource/blob/2196306/2325020/6cf921bf6234f1d8d61cff84882ececa/2024-12-11-mpk-beschluesse-errichtung-und-betrieb-noots-data.pdf?download=1.

37 COM (2016) 179 final, S. 3, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016DC0179.

38 Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 2.10.2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nummer 1024/2012.

39 Das Portal ist über diesen Link zu finden: https://europa.eu/youreurope///about/index_de.htm. Bereits jetzt enthält es hilfreiche Informationen.

40 Voigt/Rother/Sage, Die Single Digital Gateway-Verordnung: Lehren aus der Umsetzung in fünf EU-Staaten, Oktober 2024, S. 3, 20, https://www.oeffentliche-it.de/documents/10181/14412/Die+Single+Digital+Gateway-Verordnung+-+Lehren+aus+der+Umsetzung+in+fünf+EU-Staaten.

### 5. Hochschulen und Verwaltungsdigitalisierung

Auch hier gilt, staatliche Hochschulen als juristische Personen des öffentlichen Rechts müssen die Vorgaben zur Verwaltungsdigitalisierung umsetzen. Nach den Änderungen durch das OZG 2.0 sind Hochschulen noch deutlicher vom Anwendungsbereich des OZG erfasst.[41] Die Hochschulen müssen ihre Verwaltungsleistungen also elektronisch anbieten. Darunter fallen beispielsweise Gebührenbescheide oder Entscheidungen über die Bewerbung für ein Hochschulstudium, die Zulassung zur Gasthörerschaft, beantragte Im- und Exmatrikulationen und der elektronische Abruf von Bescheinigungen. Viele Hochschulen sind sehr offen für die Digitalisierung der Verwaltungsvorgänge. So bieten sie diverse Leistungen bereits elektronisch an und kommen den Vorgaben des OZG nach. Gerade die BundID bzw. zukünftige DeutschlandID wird die Beantragung von Verwaltungsleistungen im Portalverbund weiter vereinfachen und eine Nutzung durch Hochschulen bietet sich geradezu an. Die Lehre und das Abhalten von Lehrveranstaltungen sind wiederum keine elektronischen Verwaltungsleistungen, sondern fallen in den Bereich der grundrechtlich geschützten Wissenschaftsfreiheit und Freiheit der Lehre nach Art. 5 Abs. 3 S. 1 Var. 2 GG. Die Vorgaben des OZG sind dafür nicht einschlägig.[42]

Die Verwaltungsleistungen müssen aber zunächst digitalisiert werden. Für eine systematisierte Digitalisierung von Leistungen, die von den Bundesländern und Kommunen erbracht werden, verantworten das Bundesministerium des Innern und für Heimat (BMI) und die Föderale IT-Kooperation (FITKO) das „Digitalisierungsprogramm Föderal“. Für den Stand zu den einzelnen Verwaltungsleistungen existiert ein OZG-Umsetzungskatalog inklusive Informationsplattform.[43] Die Verwaltungsleistungen sind in 14 Themenfelder unterteilt. Das Themenfeld „Bildung“ bündelt die OZG-Leistungen in den vier Lebenslagen Schule, Weiterbildung, Studium und Berufsausbildung. Leistungen wie die Anerkennung von Bildungsabschlüssen zur Zulassung zu Studiengängen oder Prüfungen sind im Umsetzungsprogramm aufgenommen, aber noch nicht sehr weit. Bisher stehen nur Informationen zu dieser Leistung online und als pdf-Download zur Verfügung. Entscheidend bei der Umsetzung ist auch das Einer-für-Alle-Prinzip, wonach ein Bundesland ein digitales Verwaltungsangebot zentral entwickelt und anderen Ländern und Kommunen zur Verfügung stellt.[44]

## III. Die Verwaltungsdigitalisierung ist ein langer Prozess

Der deutsche und der europäische Gesetzgeber geben sich große Mühe, die öffentliche Verwaltung über digitale Instrumente nutzerfreundlicher zu gestalten. Die rechtlichen Vorgaben sind vielseitig und greifen ineinander. Es überrascht allerdings nicht, dass die Verwaltungsdigitalisierung selbst nach vielen Jahren kontinuierlich andauert und neue technische Entwicklungen einbeziehen muss. Gerade der Einsatz von Künstlicher Intelligenz wird in den kommenden Jahren auch ein großes Thema in der Verwaltungsdigitalisierung sein.

Staatliche Hochschulen müssen die Digitalisierungsvorgaben bezüglich ihrer Verwaltungsleistungen ebenfalls umsetzen. Dafür lohnt es sich Verantwortlichkeiten zur Umsetzung des OZG klar zu verteilen, nutzerzentriert zu arbeiten, bestehende digitale (auch nicht staatliche) Angebote für eine Integration in Hochschuldienste anzuregen und zu evaluieren.[45] Die Digitalisierung spielt auch in Studium und Lehre eine Rolle. Dort sind es statt rechtlicher Vorgaben jedoch eher konkrete Maßnahmen, die die Hochschulen ins digitale Zeitalter führen sollen.[46] Studierende würden solche Maßnahmen sehr begrüßen.[47] Die Wege zu einer digitalen Hochschule scheinen langsam geebnet.

---

41 BT-Drs. 20/8093, S. 34, https://dserver.bundestag.de/btd/20/080/2008093.pdf.

42 Vgl. Zäper, Die Verfassungsmäßigkeit des Onlinezugangsgesetzes, 2023, S. 79 f.

43 Der OZG-Katalog ist hier zu finden: https://informationsplattform.ozg-umsetzung.de/iNG/app/intro.

44 Siehe zum EfA-Prinzip bereits Yang-Jacobi, Föderal. Digital. Gut., DFN-Infobrief Recht 2/2025.

45 Hochschulforum Digitalisierung, Abschlussbericht zu Herausforderungen bei der Umsetzung des Onlinezugangsgesetzes im Kontext der Digitalen Hochschulbildung, Dezember 2020, S. 115 ff., https://hochschulforumdigitalisierung.de/sites/default/files/dateien/HFD_AP_55_Onlinezugangsgesetz_Hochschulen.pdf.

46 Vgl. die Maßnahmen des BMBF, https://www.bmbf.de/DE/Forschung/Wissenschaftssystem/Hochschulen/DigitaleHochschulbildung/digitalehochschulbildung_node.html.

47 Bitkom, Studie zur Digitalisierung an Hochschulen, 21.3.2024, https://www.bitkom.org/Presse/Presseinformation/So-digital-sind-Deutschlands-Hochschulen.

# Heute schon geNISt?

## Die Umsetzung der NIS-2-Richtlinie durch die Bundesregierung lässt weiter auf sich warten

*Von Marc-Philipp Geiselmann, Münster*

Die Network and Information Security (NIS)-2-Richtlinie (NIS-2-RL) der Europäischen Union muss nach wie vor vom deutschen Gesetzgeber umgesetzt werden, obwohl die Umsetzungsfrist seit dem 18. Oktober 2024 abgelaufen ist. Ein umfangreicher Gesetzesentwurf der Bundesregierung liegt vor, der insbesondere den Anwendungsbereich des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) stark erweitert.

## I. Hintergrund der NIS-2-RL

Cyberangriffe gefährden die Funktionsfähigkeit von Unternehmen wie Behörden. Der Gesamtschaden durch Datendiebstahl, Industriespionage oder Sabotage betrug in Deutschland im Jahr 2024 266,6 Milliarden EUR.[1] Demgegenüber stehen Ausgaben für die IT-Sicherheit in Höhe von 11,2 Milliarden EUR.[2] Die NIS-Richtlinie sollte 2016 als erste europäische Regulierung Mindestanforderungen bezüglich der Sicherheit der Netze und Informationssysteme harmonisieren und EU-weit die Zusammenarbeit der Mitgliedstaaten in Bereich der Informationssicherheit verbessern. Allerdings wurde die NIS-RL in den Mitgliedstaaten sehr unterschiedlich umgesetzt. Insbesondere der Begriff der „wesentlichen Dienste“ wurde unterschiedlich definiert, was zu einem uneinheitlichen Anwendungsbereich innerhalb der EU führte. Zudem stellte sich das Schutzniveau der NIS-RL angesichts der zunehmenden Cyberangriffe als zu niedrig heraus.[3] Anfang 2022 trat die zweite Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2-RL) anstelle der bisherigen Vorgaben in Kraft.[4]

Bis 17. Oktober 2024 sollten die EU-Mitgliedstaaten die NIS-2-Richtlinie in nationales Recht umsetzen.[5] Bislang hat die Bundesrepublik Deutschland allerdings kein Umsetzungsgesetz erlassen. Am 2. Oktober 2024 wurde der Entwurf der Bundesregierung für ein NIS-2-Umsetzungs- und Cybersicherheitstärkungsgesetz (NIS2UmsuCG) dem Bundestag zugeleitet.[6] Angesichts der im Februar durchgeführten Neuwahl wurde der Entwurf in der abgelaufenen Legislaturperiode nicht mehr verabschiedet. Dabei leitete die EU-Kommission schon Ende November gegen 23 der 27 EU-Mitgliedstaaten, darunter Deutschland, ein Vertragsverletzungsverfahren wegen der Nichteinhaltung der Umsetzungsfrist ein.[7] Jedoch wird der aktuelle Gesetzesentwurf auch in der neuen Legislatur wegen des Grundsatzes

1 Schäden durch Datendiebstahl, Industriespionage oder Sabotage in Deutschland im Jahr 2024, abrufbar unter https://de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen/, zuletzt abgerufen am 28.02.2025.

2 Ausgaben für IT-Sicherheit in Deutschland in den Jahren 2017 bis 2023 und Prognose bis 2024, abrufbar unter https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/, zuletzt abgerufen am 28.02.2025.

3 Ausführlich dazu John, CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS?, DFN-Infobrief Recht 4/2023.

4 Gitter, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Aufl. 2024, § 15 Rn. 13.

5 Vgl. Art. 41 Abs. 1 NIS-2-RL.

6 BT-Drs. 20/13184 vom 02.10.2024, abrufbar unter https://dserver.bundestag.de/btd/20/131/2013184.pdf, zuletzt abgerufen am 28.02.2025.

7 Pressemitteilung, EU-Kommission, Die Kommission fordert 23 Mitgliedstaaten auf, die NIS2-Richtlinie vollständig umzusetzen, https://digital-strategy.ec.europa.eu/de/news/commission-calls-23-member-states-fully-transpose-nis2-directive, zuletzt abgerufen am 28.02.2025.

der materiellen Diskontinuität nicht sofort, sondern erst nach neuerlichen Beratungen verabschiedet werden können.[8] Damit steigt die Wahrscheinlichkeit einer Klage der EU-Kommission vor dem Europäischen Gerichtshof (EuGH) wegen der fehlenden Umsetzung der NIS-2-RL.

## II. NIS-2-RL

Die NIS-2-Richtlinie erweitert und konkretisiert die Regelungen der NIS-Richtlinie, die im August 2016 in Kraft trat. Sie nimmt einen Wechsel vom vorherigen sektoralen Ansatz hin zu einem risikobasierten vor.[9] Insbesondere wurde der Anwendungsbereich der Richtlinie deutlich erweitert und harmonisierte Sicherheitsanforderungen wurden konkretisiert. Während der Sektor der öffentlichen Verwaltung vom Anwendungsbereich der NIS-Richtlinie noch nicht umfasst war (vgl. Art. 1 NIS-RL), erstreckt sich der erweiterte Anwendungsbereich der NIS-2-Richtlinie nun auch auf Einrichtungen der öffentlichen Verwaltung i. S. d. Art. 2 Abs. 2 lit. f Ziffer ii NIS-2-RL, Art. 6 Nr. 35 NIS-2-RL.

### 1. Gegenstand und Anwendungsbereich

Mit der NIS-2-RL soll ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden, Art. 1 Abs. 1 NIS-2-RL. Dazu werden alle Mitgliedstaaten verpflichtet, nationale Cybersicherheitsstrategien zu verabschieden sowie Behörden für das Cyberkrisenmanagement und Computer-Notfallteams zu benennen oder einzurichten, Art. 1 Abs. 2 lit. a NIS-2-RL. Einrichtungen, die von der NIS-2-RL erfasst sind, werden zudem Pflichten in Bezug auf das Cybersicherheitsrisikomanagement sowie Berichtspflichten auferlegt, Art. 1 Abs. 2 lit. b NIS-2-RL. Außerdem werden Vorschriften zum Austausch von Cybersicherheitsinformationen sowie Aufsichts- und Durchsetzungspflichten für die Mitgliedsstaaten implementiert.

Für die Bestimmung der von der Richtlinie erfassten Einrichtungen verweist Art. 2 Abs. 1 NIS-2-RL auf den Anhang I und II der Richtlinie. Im Anhang I sind elf Sektoren mit hoher Kritikalität aufgeführt, die sich wiederum in Teilsektoren und verschiedene Arten der jeweiligen Einrichtungen untergliedern. Dabei handelt es sich um Energie (Nr. 1), Verkehr (Nr. 2), Bankwesen (Nr. 3), Finanzmarktinfrastrukturen (Nr. 4), Gesundheitswesen (Nr. 5), Trinkwasser (Nr. 6), Abwasser (Nr. 7), digitale Infrastruktur (Nr. 8), Verwaltung von IKT-Diensten (Business-to-Business) (Nr. 9), öffentliche Verwaltung (Nr. 10) und Weltraum (Nr. 11). Im Anhang II sind sieben sonstige kritische Sektoren aufgelistet. Das sind Post- und Kurierdienste (Nr. 1), Abfallbewirtschaftung (Nr. 2), Produktion, Herstellung und Handel mit chemischen Stoffen (Nr. 3), Produktion, Verarbeitung und Vertrieb von Lebensmitteln (Nr. 4), Verarbeitendes Gewerbe/ Herstellung von Waren (Nr. 5), Anbieter digitaler Dienste (Nr. 6) und Forschung (Nr. 7). Der Begriff der Forschungseinrichtung ist nach Art. 6 Nr. 41 NIS-2-RL als Einrichtung definiert, deren primäres Ziel es ist, die angewandte Forschung oder die experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen, die jedoch Bildungseinrichtungen nicht einschließt. Die Einrichtungen sind jedoch nur betroffen, sofern sie nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 jenes Artikels überschreiten. Das bedeutet, dass die Einrichtung 50 oder mehr Personen beschäftigt oder der Jahresumsatz der Einrichtung 10 Mio. EUR oder mehr betragen muss. Der Art. 2 Abs. 2 bis 4 NIS-2-RL listet Einrichtungen auf, die unabhängig von ihrer Größe erfasst sind. Die Mitgliedstaaten können zudem kommunale Einrichtungen und Bildungseinrichtungen miteinbeziehen, Art. 2 Abs. 5 NIS-2-RL. [10]

Art. 3 NIS-2-RL unterteilt die Einrichtungen anschließend nochmals in wesentliche und wichtige Einrichtungen. Wesentlich sind die Einrichtungen der in Anhang I aufgeführten Art, die die in Artikel 2 Absatz 1 des Anhangs der Empfehlung 2003/361/EG genannten Schwellenwerte für mittlere Unternehmen überschreiten. Das bedeutet, dass die Einrichtungen 250 oder mehr Personen beschäftigen oder einen Jahresumsatz von mehr als 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf mehr als 43 Mio. EUR belaufen muss. In Art. 3 Abs. 1 lit. b bis g NIS-2-RL sind weitere Einrichtungen unabhängig von ihrer Größe aufgelistet. Alle weiteren in Anhang I und II aufgeführten Unternehmen, die nicht als wesentliche Einrichtungen gelten, gelten als wichtige Einrichtungen.

8 Magiera, in: Sachs, 10. Aufl. 2024, GG, Art. 39 Rn. 15.

9 Bostelmann, in: Hornung/Schallbruch, IT-Sicherheitsrecht, §25 Rn. 17.

10 Gitter, in: Hornung/Schallbruch, IT-Sicherheitsrecht, §15 Rn. 13 ff.

## 2. Cybersicherheitsstrategie

Gemäß Artikel 7 obliegt es jedem Mitgliedstaat, eine nationale Cybersicherheitsstrategie zu erlassen, welche die strategischen Ziele definiert und die zur Erreichung dieser Ziele notwendigen Ressourcen sowie angemessene politische und regulatorische Maßnahmen umfasst. Diese Strategie muss insbesondere die Ziele und Prioritäten im Bereich der Cybersicherheit abbilden, die in den Anhängen genannten Sektoren berücksichtigen und einen Steuerungsrahmen zur Erreichung dieser Ziele festlegen, Art. 7 Abs. 1 lit. a und b NIS-2-RL. Der Steuerungsrahmen soll die Aufgaben und Zuständigkeiten der nationalen Interessenträger klarstellen und die Koordination sowohl auf nationaler Ebene als auch mit den sektorspezifisch zuständigen Behörden der Union sicherstellen, Art. 7 Abs. 1 lit. c NIS-2-RL. Weiterhin sieht die Strategie Mechanismen zur Risikoermittlung und -bewertung vor, um Vorsorge, Reaktionsfähigkeit und Wiederherstellung im Falle von Sicherheitsvorfällen zu gewährleisten, Art. 7 Abs. 1 lit. d und e NIS-2-RL. Eine Liste der beteiligten Behörden und Interessenträger ist zu erstellen, und es sind Maßnahmen zur Förderung der Cybersicherheits-Sensibilisierung der Bürger zu ergreifen, Art. 7 Abs. 1 lit. f und h NIS-2-RL.

Im Rahmen der nationalen Cybersicherheitsstrategie müssen Mitgliedstaaten Konzepte entwickeln, die insbesondere die Sicherheit in der Lieferkette von IKT-Produkten und -Diensten betreffen, Art. 7 Abs. 2 lit. a NIS-2-RL. Dies schließt die Spezifikation von Cybersicherheitsanforderungen bei öffentlichen Aufträgen ein, etwa zur Zertifizierung, Verschlüsselung und Nutzung quelloffener Produkte, Art. 7 Abs. 2 lit. b NIS-2-RL. Zudem sind Maßnahmen zur koordinierten Offenlegung von Schwachstellen und zur Sicherstellung der Integrität und Vertraulichkeit des öffentlichen Internets, einschließlich Unterseekabel, erforderlich, Art. 7 Abs. 2 lit. c und d NIS-2-RL. Die Strategie fördert den Einsatz fortschrittlicher Technologien, die Bildung und Sensibilisierung im Bereich Cybersicherheit sowie die Unterstützung von Hochschulen bei der Verbesserung der Cybersicherheitsinstrumente und -infrastruktur, Art. 7 Abs. 2 lit. e bis g NIS-2-RL. Ein effektiver Informationsaustausch zwischen Einrichtungen soll gewährleistet werden und die Cyberresilienz von kleinen und mittleren Unternehmen ist zu stärken, insbesondere von solchen außerhalb des Anwendungsbereichs der Richtlinie, Art. 7 Abs. 2 lit. h und i NIS-2-RL. Abschließend wird die Förderung eines aktiven Cyberschutzes angestrebt, Art. 7 Abs. 2 lit. j NIS-2-RL.

Die Mitgliedstaaten sind verpflichtet, ihre Cybersicherheitsstrategien innerhalb von drei Monaten nach deren Erlass der Europäischen Kommission zu notifizieren, wobei auf nationale Sicherheitsbelange bezogene Informationen ausgenommen werden können, Art. 7 Abs. 3 NIS-2-RL. Eine regelmäßige, mindestens alle fünf Jahre durchzuführende Bewertung und gegebenenfalls Aktualisierung der Strategien anhand wesentlicher Leistungsindikatoren wird vorgeschrieben. Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) steht den Mitgliedstaaten auf Anfrage beratend zur Seite, um die Strategie konform mit den Richtlinienanforderungen anzupassen oder zu aktualisieren, Art. 7 Abs. 4 NIS-2-RL.

## 3. Behörden für das Cyberkrisenmanagement

Gemäß Art. 9 NIS-2-RL muss jeder Mitgliedstaat eine oder mehrere Behörden ernennen oder einrichten, die für das Management von Cybersicherheitsvorfällen großen Ausmaßes zuständig sind. Diese Behörden sind mit angemessenen Ressourcen auszustatten und sollen im Einklang mit bestehenden nationalen Krisenmanagementsystemen arbeiten. Sollte es mehrere solche Behörden geben, muss eine als Koordinator benannt werden, Art. 9 Abs. 1 f. NIS-2-RL.

Zudem hat jeder Mitgliedstaat die notwendigen Kapazitäten, Mittel und Verfahren zu identifizieren und einen nationalen Reaktionsplan zu entwickeln, Art. 9 Abs. 3 NIS-2-RL. Darüber hinaus ist ein nationaler Plan zu verabschieden, der die Ziele und Verfahren des Cyberkrisenmanagements festlegt, die Verantwortlichkeiten der zuständigen Behörden klärt, die Verfahren in den nationalen Krisenmanagementrahmen integriert und relevante Interessenträger sowie Infrastrukturen berücksichtigt, Art. 9 Abs. 4 NIS-2-RL.

Die Mitgliedstaaten sind verpflichtet, der Europäischen Kommission innerhalb von drei Monaten die Identität der zuständigen Behörde zu melden und relevante Informationen über ihre Reaktionspläne bereitzustellen. Informationen können ausgeschlossen werden, wenn dies für die nationale Sicherheit erforderlich ist, Art. 9 Abs. 5 NIS-2-RL.

### 4. Computer-Notfallteams (CSIRTs)

Jeder Mitgliedstaat muss nach Art. 10 NIS-2-RL ein oder mehrere Computer-Notfallteams (CSIRTs) benennen oder einrichten, die die Anforderungen der Richtlinie erfüllen und für bestimmte Sektoren zuständig sind, Art. 10 Abs. 1 NIS-2-RL. Diese CSIRTs erhalten ausreichende Ressourcen und eine sichere Kommunikationsinfrastruktur für den Informationsaustausch mit wichtigen Einrichtungen und anderen Akteuren, Art. 10 Abs. 2 f. NIS-2-RL. Sie arbeiten mit sektorenübergreifenden Einrichtungen zusammen, nehmen an Peer Reviews teil und kooperieren innerhalb des CSIRTs-Netzwerks, Art. 10 Abs. 4 bis 6 NIS-2-RL. Auch Beziehungen zu nationalen Computer-Notfallteams von Drittländern können aufgenommen werden, um einen effektiven Informationsaustausch zu ermöglichen, Art. 10 Abs. 7 f. NIS-2-RL. Die Mitgliedstaaten müssen der Europäischen Kommission die Identität und Aufgaben der CSIRTs mitteilen und haben die Möglichkeit, bei der Einrichtung der CSIRTs Unterstützung von der ENISA zu erhalten, Art. 10 Abs. 9 f. NIS-2-RL.

## III. Gesetzesentwurf der Bundesregierung

Um die NIS-2-RL umzusetzen, sieht der Entwurf des NIS2UmsuCG insbesondere umfangreiche Änderungen am BISG vor.

### Änderungen des BSIG

Der Entwurf der von der Ampelkoalition getragenen Bundesregierung sieht wesentliche Änderungen des BSIG vor. Statt der bisherigen 14 Paragrafen beinhaltet das BSIG-E der Bundesregierung 65 Paragrafen.

Kernstück des Gesetzesentwurfs ist Teil 3, der die Sicherheit in der Informationstechnik von Einrichtungen regelt. In diesem wird zunächst der Anwendungsbereich des BSIG deutlich erweitert. War dieser bisher auf Betreiber kritischer Infrastrukturen, Anbieter digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse beschränkt, so führt der Entwurf der Bundesregierung für das NIS2UmsuCG die durch die NIS-2-RL vorgegebenen Einrichtungskategorien „besonders wichtige Einrichtungen und wichtige Einrichtungen“ ein. Dies schließt in Summe deutlich mehr Unternehmen ein.[11] Zudem führt § 28 Abs. 7 BSIG-E die neue Kategorie der Betreiber kritischer Anlagen ein. Der Begriff der kritischen Anlage wird in § 2 Nr. 22 BSIG-E legaldefiniert und meint demnach Anlagen, die für die Erbringung einer kritischen Dienstleistung erheblich sind. Gem. § 29 Abs. 1, 2 BSIG-E sind auf Einrichtungen der Bundesverwaltung, mit wenigen Ausnahmen, die Regelungen für besonders wichtige Einrichtungen anzuwenden.

In § 30 BSIG-E finden sich die Mindestsicherheitsanforderungen des Art. 21 Abs. 2 NIS-2-Richtlinie als Risikomanagementmaßnahmen für besonders wichtige Einrichtungen und wichtige Einrichtungen. Diese sind gem. § 30 Abs. 1 BSIG-E dazu verpflichtet, „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen […] zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden […].“ § 30 Abs. 2 BSIG-E konkretisiert die Mindestanforderungen an die zu ergreifenden technischen und organisatorischen Maßnahmen.

Mit der Klassifizierung als besonders wichtige oder wichtige Einrichtung gem. § 28 BSIG-E gehen außerdem auch Melde-, Registrierungs- und Unterrichtungspflichten einher, welche die §§ 32 ff. BSIG-E umsetzen. Darüber hinaus kommen den Geschäftsleitungen entsprechender Einrichtungen Umsetzungs-, Überwachungs- und Schulungspflichten zu, § 38 BSIG-E. Statt wie bisher alle zwei Jahre sollen Betreiber kritischer Anlagen gem. § 39 BSIG-E nur noch alle drei Jahre die Umsetzung der technischen und organisatorischen Maßnahmen i. S. d. § 30 BSIG-E nachweisen müssen.

## IV. Relevanz für Hochschulen

Die Umsetzung der NIS-2-Richtlinie wird sich in Deutschland aufgrund der vorgezogenen Bundestagswahl im Februar noch verzögern. Jedoch hat die EU-Kommission bereits ein Vertragsverletzungsverfahren initiiert, sodass die Umsetzung eilt. Dass sich der neue Bundestag den Gesetzesentwurf der von der Ampelkoalition getragenen Bundesregierung von Oktober 2024 in weiten Teilen zu eigen machen wird, ist deshalb nicht unwahrscheinlich. Dieser allerdings sieht keine Übergangsfristen

11 Schmidt, RDi 2024, 550, 550 f.

vor, sodass sich bereits jetzt die Prüfung lohnt, ob eine Einrichtung von dem Anwendungsbereich der NIS-2-RL betroffen ist.[12]

Die NIS-2-RL erfasst Forschungseinrichtungen in Anhang II Nr. 7 als sonstige kritische Einrichtungen. In der Definition der Forschungseinrichtungen in Art. 6 Nr. 41 NIS-2-RL werden Bildungseinrichtungen allerdings ausgeschlossen. Dennoch können die Mitgliedstaaten nach Art. 2 Abs. 5 lit. b NIS-2-RL vorsehen, dass die Richtlinie auf Bildungseinrichtungen Anwendung findet, insbesondere, wenn sie kritische Forschungstätigkeiten durchführen.

Auch § 2 Nr. 12 BSIG-E übernimmt diese Definition, welche Bildungseinrichtungen von der Definition der Forschungseinrichtungen ausnimmt. In der Stellungnahme des Nationalen Normenkontrollrates, der dem Gesetzesentwurf als Anlage 2 beigefügt ist, ist aufgeführt, dass der Gesetzentwurf einem Beschluss des IT-Planungsrates (2023/39) folgt, der den Bund auffordert, Bildungseinrichtungen aus dem Anwendungsbereich des nationalen Umsetzungsgesetzes auszunehmen.

Dementsprechend kann davon ausgegangen werden, dass Hochschulen wohl nicht vom Anwendungsbereich der NIS-2-RL umfasst sind.

Universitätskliniken hingegen fallen in den Anwendungsbereich der NIS-2-RL. Sie sind im Anhang I Sektor 5 Gesundheitswesen aufgeführt. Dieser nennt als Art der Einreichung Gesundheitsdienstleister im Sinne des Art. 3 lit. g der RL 2011/24/EU des Europäischen Parlaments und des Rates. Dieser wiederum definiert als „Gesundheitsdienstleister“ jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt.

## V. Fazit

Die NIS-2-RL entwickelt das IT-Sicherheitsniveau in der Europäischen Union weiter und erhöht die Mindestanforderungen für die IT-Sicherheit. Auch wenn Unternehmen oder Einrichtungen nicht von der NIS-2-RL umfasst sind, ist es empfehlenswert, sich mit der IT-Sicherheit zu befassen und in sie zu investieren. Eine Möglichkeit, wie dies geschehen kann, zeigt der Entwurf des Landes Nordrhein-Westfalen für ein Hochschulstärkungsgesetz: Nach § 8b Hochschulgesetz-NRW-E haben Hochschulen einen Chief Information Officer (CIO) und einen Chief Information Security Officer (CISO) zu bestellen.[13] Diese haben ihre Ämter hauptamtlich zu führen, die IT-Strategie der Hochschule fortzuentwickeln und müssen Regelungen zur Informationssicherheit erlassen. Dazu werden ihnen über den Landeshaushalt entsprechende Mittel bereitgestellt. Sie haben schließlich über eine angemessene Qualifikation und Berufserfahrung zu verfügen.

12 Schmidt, RDi 2024, 550 (556).

13 Entwurf eines Gesetzes betreffend die Stärkung der Hochschullandschaft (Hochschulstärkungsgesetz), Vorlage 18/3086, abrufbar unter https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV18-3086.pdf, zuletzt abgerufen am 28.02.2025.

# KI-Modelle made in Europe?

## Ein europäisches Forschungs-Konsortium arbeitet derzeit an mehreren Open-Source-Sprachmodellen

*Von Philipp Schöbel, Berlin*

Das neue europäische Sprachmodell trägt den Namen OpenEuroLLM und soll allen Bürger:innen, Unternehmen und öffentlichen Verwaltungen zur Verfügung gestellt werden.[1] Dabei wird die EU-Rechtskonformität des Modells betont. So sollen auch Hochschulen künftig ein rechtskonformes Large Language Model (LLM)[2] nutzen können. Das bedeutet aber auch, dass insbesondere die Vorschriften aus dem Artificial Intelligence Act (AI Act) bei der Erstellung des Modells eingehalten werden müssen. Der AI Act ist im Infobrief schon mehrfach besprochen worden.[3] Bisher lag der Schwerpunkt jedoch auf den Regelungen für KI-Systeme. Die Regelungen zu KI-Modellen sollen in diesem Beitrag näher beleuchtet werden.

## I. Warum europäische Sprachmodelle?

Die erfolgreichsten großen Sprachmodelle kommen derzeit aus dem außereuropäischen Ausland. Bisher ist unklar, ob deren Entwicklung im Einklang mit dem europäischen Urheber-, Datenschutz- und Produktsicherheitsrecht steht. Die EU will eine europäische Alternative fördern, die neben der rechtlichen Compliance noch weitere Vorteile bietet. An der Entwicklung von OpenEuroLLM sind 20 Forschungsinstitute, Universitäten und Unternehmen aus ganz Europa beteiligt.[4] Ziel ist es, leistungsfähige, mehrsprachige, große Sprachgrundlagenmodelle für kommerzielle, industrielle und öffentliche Dienstleistungen bereitzustellen.[5]

Das LLM soll dabei alle offiziellen und zukünftigen Sprachen der EU-Mitgliedstaaten abdecken.[6] Daneben soll etwa auch mit Hindi und Arabisch trainiert werden.[7] Bisher sind die gängigen Sprachmodelle zwar in der Lage mit anderen Sprachen als Englisch zu arbeiten, aber leisten keine vergleichbaren Ergebnisse. Gerade für Sprachen, die weniger Menschen sprechen, rechnet sich das Training von großen Sprachmodellen derzeit nicht.[8] Dieser Benachteiligung will die EU mit eigenen Modellen

1 Handelsblatt, Bis zu 54 Millionen Euro für eine Europa-KI, 04.02.2025, abrufbar unter: https://www.handelsblatt.com/technik/ki/eu-kommission-bis-zu-54-millionen-euro-fuer-eine-europa-ki/100104475.html, alle Internetquellen wurden zuletzt am 11.02.2025 abgerufen.

2 Zum Personenbezug in LLMs siehe Müller, Das kann sich doch niemand merken, DFN-Infobrief Recht 03 / 2025, S. 7.

3 Schöbel, Europäische Sandkästen für KI, DFN-Infobrief Recht 8 / 2024, S. 2; Schöbel, AI Act – Licht der Europäischen Union?, DFN-Infobrief Recht 12 / 2024, S. 7; Schöbel, Der AI Act und die Wissenschaft, DFN-Infobrief Recht 2 / 2025, S. 2.

4 t3n, Europas Antwort auf ChatGPT und Deepseek: OpenEuroLLM stellt sich vor, 09.02.2025, abrufbar unter: https://t3n.de/news/europas-antwort-auf-chatgpt-und-deepseek-openeurollm-1671257/.

5 OpenEuroLLM, Pressemitteilung vom 03.02.2025, abrufbar unter: https://openeurollm.eu/launch-press-release.

6 Europäische Kommission, Pressemitteilung vom 03.02.2025, abrufbar unter: https://digital-strategy.ec.europa.eu/de/news/pioneering-ai-project-awarded-opening-large-language-models-european-languages.

7 Heise, Sprachmodell: OpenEuroLLM soll KI in der EU unabhängiger und vielfältiger machen, 04.02.2025, abrufbar unter: https://www.heise.de/news/Sprachmodell-OpenEuroLLM-soll-KI-in-der-EU-unabhaengiger-und-vielfaeltiger-machen-10269667.html.

8 Handelsblatt, Bis zu 54 Millionen Euro für eine Europa-KI, 04.02.2025, abrufbar unter: https://www.handelsblatt.com/technik/ki/eu-kommission-bis-zu-54-millionen-euro-fuer-eine-europa-ki/100104475.html.

entgegenwirken. Im vergangenen November war bereits mit „Teuken-7B“ ein Sprachmodell veröffentlicht worden, das mit den 24 Amtssprachen der EU trainiert wurde.[9] Auch dieses Modell wurde von einem Forschungskonsortium entwickelt.

OpenEuroLLM wird nicht das erste Open-Source-LLM sein. Neu wird aber der Grad der Offenheit des Modells sein. Die Entwickler:innen wollen nicht nur den Code der Modelle, die zugehörige Software und die Evaluierung für alle gänzlich offen zugänglich machen. Im Gegensatz zu anderen Open-Source-LLMs sollen auch die Trainingsdaten öffentlich zugänglich sein.[10]

## II. Was ist ein KI-Modell?

Ein KI-Modell kann als parametrisiertes (Computer-)Programm verstanden werden, d.h. die Parameter werden durch einen automatisierten (Lern-)Prozess, ggf. unter Zuhilfenahme von Trainingsdaten, ermittelt.[11] Die ermittelten Parameter und das zugehörige Programm bilden das KI-Modell.[12]

Im Gegensatz zu KI-Systemen sind KI-Modelle nicht in der KI-Verordnung (KI-VO) legaldefiniert. In den Erwägungsgründen der Verordnung wird davon ausgegangen, dass KI-Modelle wesentliche Komponenten von KI-Systemen sind, aber für sich genommen keine KI-Systeme darstellen. „KI-Modelle sind in der Regel in KI-Systeme integriert und Teil davon.“[13] Damit ein KI-Modell zu einem KI-System wird, müssen weitere Komponenten hinzugefügt werden. Ein Beispiel hierfür ist etwa das Einfügen einer Nutzerschnittstelle. Während also etwa ChatGPT ein KI-System darstellt, ist das zugrundeliegende LLM GPT-4 ein KI-Modell im Sinne der KI-VO.

## III. Welche Arten von KI-Modellen werden reguliert?

Durch die KI-VO werden nicht alle Arten von KI-Modellen reguliert. Da beim damaligen Rechtsetzungsverfahren die rasante Entwicklung von ChatGPT prägend war, beschränkt sich die Regulierung auf KI-Modelle mit allgemeinem Verwendungszweck und KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko. Es wird also zwischen zwei Arten von regulierten KI-Modellen unterschieden: solchen mit allgemeinem Verwendungszweck und solchen, die zusätzlich ein systemisches Risiko bergen.

Für die Einstufung eines KI-Modells mit allgemeinem Verwendungszweck muss das Modell drei Kriterien kumulativ erfüllen[14]: Es muss eine erhebliche allgemeine Verwendbarkeit aufweisen, ein breites Spektrum unterschiedlicher Aufgaben kompetent erfüllen können und in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden können. KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden, sind ausgenommen.[15] Das Europäische Amt für künstliche Intelligenz (KI-Büro) will konkretisierende Erläuterungen zu dem Begriff des KI-Modells mit allgemeinem Verwendungszweck erstellen.[16]

Systemisch ist ein Risiko, das speziell mit den Fähigkeiten von KI-Modellen mit großer Wirkung verbunden ist. Dazu muss es aufgrund der Reichweite oder aufgrund vorhersehbarer negativer Folgen erhebliche Auswirkungen auf den Unionsmarkt haben. Diese Auswirkungen müssen sich in großem Maßstab über die Wertschöpfungskette ausbreiten können. Negative Folgen sind solche für die öffentliche Gesundheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt.[17]

---

9 Fraunhofer IAIS, Presseinformation, 26.11.2024, abrufbar unter: https://www.iais.fraunhofer.de/de/presse/presseinformationen/presseinformationen-2024/presseinformation-241126.html.

10 Heise, Sprachmodell: OpenEuroLLM soll KI in der EU unabhängiger und vielfältiger machen, 04.02.2025, abrufbar unter: https://www.heise.de/news/Sprachmodell-OpenEuroLLM-soll-KI-in-der-EU-unabhaengiger-und-vielfaeltiger-machen-10269667.html.

11 Bender, Automatisierte Verarbeitung natürlicher Sprache im Kontext von KI-Modellen, KIR 2025, 3, 4.

12 Bender, Automatisierte Verarbeitung natürlicher Sprache im Kontext von KI-Modellen, KIR 2025, 3, 4.

13 Erwg. 97 KI-VO.

14 Art. 3 Nr. 63 KI-VO.

15 Art. 3 Nr. 63 KI-VO.

16 Europäische Kommission, KI-Modelle für allgemeine Zwecke im KI-Gesetz – Fragen und Antworten, Frage 2, abrufbar unter: https://digital-strategy.ec.europa.eu/de/faqs/general-purpose-ai-models-ai-act-questions-answers.

17 Art. 3 Nr. 65 KI-VO.

## IV. Wie wird beurteilt, ob ein systemisches Risiko vorliegt?

Ein systemisches Risiko liegt bei einem KI-Modell mit allgemeinem Verwendungszweck vor, wenn es eine von zwei alternativen Bedingungen erfüllt:
Nach der ersten Alternative muss das KI-Modell über Fähigkeiten mit hohem Wirkungsgrad verfügen.[18] Fähigkeiten mit hoher Wirkkraft bezeichnet Fähigkeiten, die denen der fortschrittlichsten KI-Modelle mit allgemeinem Verwendungszweck entsprechen oder diese Fähigkeiten übersteigen.[19] Dies wird angenommen, wenn die kumulierte Menge der für das Training des KI-Modells mit allgemeinem Verwendungszweck verwendeten Berechnungen, gemessen in Gleitkommaoperationen, mehr als 1025 beträgt. [20] Der Schwellenwert kann von der Kommission per delegiertem Rechtsakt[21] geändert werden.[22]

Nach der zweiten Alternative kann die Kommission von Amts wegen oder aufgrund einer qualifizierten Warnung des wissenschaftlichen Gremiums entscheiden, dass ein KI-Modell – unabhängig von der Berechnungsanzahl - über Fähigkeiten oder eine Wirkung verfügt, die denen der ersten Alternative entsprechen.[23] Die Kommission ist dabei an einen Katalog von Kriterien gebunden. Diese Kriterien umfassen unter anderem die Anzahl der Parameter des Modells, die Qualität oder Größe des Datensatzes und die Zahl der registrierten Endnutzer.[24] Die Kommission kann diese Kriterien per delegiertem Rechtsakt ändern. [25]

## V. Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

Anbieter[26] von KI-Modellen haben eine Reihe von Pflichten. Sie müssen die technische Dokumentation des Modells erstellen und aktualisieren.[27] Das umfasst Trainings- und Testverfahren und deren Ergebnisbewertung. Diese Dokumentation muss festgelegte Mindestangaben enthalten. Darunter fallen etwa eine allgemeine Beschreibung des KI-Modells einschließlich der Aufgaben, die das Modell erfüllen soll, sowie der Art und des Wesens der KI-Systeme, in die es integriert werden kann.[28] Darüber hinaus müssen unter anderem auch die technischen Mittel (zum Beispiel Betriebsanleitungen, Infrastruktur, Instrumente), die für die Integration des KI-Modells mit allgemeinem Verwendungszweck in KI-Systeme erforderlich sind, beschrieben werden.[29] Ebenfalls anzugeben sind die für das Trainieren des Modells verwendeten Rechenressourcen (zum Beispiel Anzahl der Gleitkommaoperationen), die Trainingszeit und andere relevante Einzelheiten im Zusammenhang mit dem Training.[30] Beschrieben werden muss auch der bekannte oder geschätzte Energieverbrauch des Modells.[31] Diese Informationen sollen dem KI-Büro und den zuständigen nationalen Behörden auf

18 Art. 51 Abs. 1 lit. a KI-VO.

19 Art. 3 Nr. 64 KI-VO.

20 Art. 51 Abs. 2 KI-VO.

21 Durch einen delegierten Rechtsakt kann die Kommission Ergänzungen oder Änderungen zu Abschnitten eines Rechtsakts erlassen (Art. 290 AEUV).

22 Art. 51 Abs. 3 KI-VO.

23 Art. 51 Abs. 1 lit. b KI-VO.

24 Anhang XIII KI-VO.

25 Art. 52 Abs. 4 UAbs. 2 KI-VO.

26 Zum Begriff des Anbieters siehe Schöbel, AI Act – Licht der Europäischen Union?, DFN-Infobrief Recht 12 / 2024, S. 7.

27 Art. 53 Abs. 1 lit. a KI-VO.

28 Anhang XI Nr. 1 lit. a KI-VO.

29 Anhang XI Nr. 2 lit. a KI-VO.

30 Anhang XI Nr. 2 lit. d KI-VO.

31 Anhang XI Nr. 2 lit. e KI-VO.

Anfrage zur Verfügung gestellt werden können.[32] Die festgelegten Mindestanforderungen an die Dokumentation können von der Kommission per delegiertem Rechtsakt geändert werden.[33] Sofern Anbieter von KI-Systemen beabsichtigen, das KI-Modell mit allgemeinem Verwendungszweck in ihre KI-Systeme zu integrieren, müssen die KI-Modell-Anbieter eine zweite Dokumentation erstellen.[34] Die bereitgestellten Informationen sollen die Anbieter von KI-Systemen in die Lage versetzen, die Fähigkeiten und Grenzen des KI-Modells gut zu verstehen und ihren Pflichten gemäß der KI-VO nachzukommen.[35] Die Mindestanforderungen an die Informationen sind in Anhang XII KI-VO festgelegt. Sie müssen unter anderem eine allgemeine Beschreibung des KI-Modells einschließlich der Aufgaben, die das Modell erfüllen soll, sowie der Art und des Wesens der KI-Systeme, in die es integriert werden kann, enthalten.[36] Zusätzlich müssen die Bestandteile des Modells und seines Entwicklungsprozesses beschrieben werden. Diese umfassen beispielsweise die technischen Mittel (Betriebsanleitungen, Infrastruktur, Instrumente, u. a.), die für die Integration des KI-Modells mit allgemeinem Verwendungszweck in KI-Systeme erforderlich sind.[37] Auch hier können die festgelegten Mindestanforderungen von der Kommission per delegiertem Rechtsakt geändert werden.[38]

Die dargestellten Dokumentations- und Informationspflichten gelten nicht für KI-Modelle, die im Rahmen einer freien und quelloffenen Lizenz bereitgestellt werden.[39] Damit diese Open-Source-Ausnahme greift, müssen eine Reihe von Anforderungen erfüllt werden. Dazu zählen, dass Zugang, Nutzung, Änderung und Verbreitung des Modells ermöglicht werden und deren Parameter, einschließlich Gewichte, Informationen über die Modellarchitektur und Informationen über die Modellnutzung, öffentlich zugänglich gemacht werden.[40] Die Ausnahme gilt nicht für KI-Modelle mit allgemeinem Verwendungszweck, wenn sie ein systemisches Risiko bergen.[41]

Die Anbieter sollen eine Strategie zur Einhaltung des Urheberrechts der Union[42] und damit zusammenhängender Rechte auf den Weg bringen.[43] Diese umfasst etwa Methoden zur Ermittlung und Einhaltung von Nutzungsvorbehalten der Rechteinhaber gegen Text und Data Mining.[44]

Außerdem müssen sie eine hinreichend detaillierte Zusammenfassung der für das Training des KI-Modells mit allgemeinem Verwendungszweck verwendeten Inhalte erstellen und veröffentlichen.[45] Hierfür soll das KI-Büro eine Vorlage bereitstellen. Wo genau die Zusammenfassung veröffentlicht werden muss, bestimmt die KI-VO nicht.[46] In der Fachliteratur wird vertreten, dass die Zusammenfassung der verwendeten Inhalte auf der Website des Anbieters (nicht versteckt) zu veröffentlichen ist.[47] Anbieter, die in Drittländern niedergelassen sind, benennen vor dem Inverkehrbringen eines KI-Modells mit allgemeinem Verwendungszweck auf dem Unionsmarkt schriftlich einen in der Union

32 Art. 53 Abs. 1 lit a KI-VO.

33 Art. 53 Abs. 6 KI-VO.

34 Art. 53 Abs. 1 lit. b S. 1 KI-VO.

35 Art. 53 Abs. 1 lit. b S. 2 i) KI-VO.

36 Anhang XII Nr. 1 lit. a KI-VO.

37 Anhang XIII Nr. 2 lit. a KI-VO.

38 Art. 53 Abs. 6 KI-VO.

39 Art. 53. Abs. 2 S. 1 KI-VO.

40 Art. 53. Abs. 2 S. 1 KI-VO.

41 Art. 53. Abs. 2 S. 2 KI-VO.

42 Zum Training von KI-Modellen mit urheberrechtlich geschützten Daten siehe Müller, Die Menge machť s, DFN-Infobrief Recht 11 / 2024, S. 2.

43 Art. 53 Abs. 1 lit. c KI-VO.

44 Bernsteiner/Schmitt, in: Martini/Wendehorst (Hrsg.), KI-VO Kommentar, Art. 53, Rn. 38.

45 Art. 53 Abs. 1 lit. d KI-VO.

46 Vgl. Bernsteiner/Schmitt, in: Martini/Wendehorst (Hrsg.), KI-VO Kommentar, Art. 53, Rn. 44.

47 Bernsteiner/Schmitt, in: Martini/Wendehorst (Hrsg.), KI-VO Kommentar, Art. 53, Rn. 44.

niedergelassenen Bevollmächtigten.[48] Der Anbieter muss seinem Bevollmächtigten ermöglichen, die Aufgaben wahrzunehmen, die in seinem Auftrag festgelegt sind.[49] Der Bevollmächtigte stellt dem KI-Büro auf Anfrage eine Kopie des Auftrags bereit.[50] An den Inhalt des Auftrags sind Mindestanforderungen gestellt. Diese umfassen zum Beispiel die Bereitstellung sämtlicher zum Nachweis der Einhaltung der dargestellten Pflichten erforderlichen Informationen und Dokumentation.[51] Mit dem Auftrag wird der Bevollmächtigte ermächtigt, neben oder anstelle des Anbieters als Ansprechpartner für das KI-Büro oder die zuständigen nationalen Behörden in allen Fragen zu dienen, die die Gewährleistung der Einhaltung dieser Verordnung betreffen.[52] Auch die Pflichten bezüglich des Bevollmächtigten gelten nicht für Open-Source-KI-Modelle.[53]

## VI. Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko

Für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko gelten zusätzliche Pflichten. Sie müssen eine Modellbewertung mit standardisierten Protokollen und Instrumenten durchführen, um systemische Risiken zu ermitteln und zu mindern.[54] Diese Bewertung muss dem Stand der Technik entsprechen. Dazu gehört auch die Durchführung und Dokumentation von Angriffstests beim Modell. Die Pflicht ist zeitlich nicht beschränkt und es ist kein Wiederholungsintervall vorgeschrieben.[55]

Eine weitere Pflicht ist die Bewertung und Minderung möglicher systemischer Risiken auf Unionsebene, die sich aus der Entwicklung, dem Inverkehrbringen oder der Nutzung von KI-Modellen mit systemischem Risiko ergeben können.[56] Dies umfasst auch die Bewertung und Minderung der Ursachen dieser Risiken. Die Bewertung soll fortlaufend erfolgen.[57] Ein genaues Bewertungsintervall ist nicht vorgeschrieben.[58]

Einschlägige Informationen über schwerwiegende Vorfälle und mögliche Abhilfemaßnahmen müssen erfasst und dokumentiert werden.[59] Das KI-Büro und gegebenenfalls die zuständigen nationalen Behörden sind unverzüglich über die schwerwiegenden Vorfälle zu unterrichten. Ein Vorfall oder eine Fehlfunktion sind schwerwiegend, wenn direkt oder indirekt eine der nachstehenden Folgen eintreten:

a) der Tod oder die schwere gesundheitliche Schädigung einer Person;

b) eine schwere und unumkehrbare Störung der Verwaltung oder des Betriebs kritischer Infrastrukturen;

c) die Verletzung von Pflichten aus den Unionsrechtsvorschriften zum Schutz der Grundrechte;

d) schwere Sach- oder Umweltschäden.[60]

48 Art. 54 Abs. 1 KI-VO.

49 Art. 54 Abs. 2 KI-VO.

50 Art. 54 Abs. 3 S. 2 KI-VO.

51 Art. 54 Abs. 3 S. 3 lit. c KI-VO.

52 Art. 54 Abs. 4 KI-VO.

53 Art. 54 Abs. 6 KI-VO.

54 Art. 55 Abs. 1 lit. a KI-VO.

55 Bernsteiner/Schmitt, in: Martini/Wendehorst (Hrsg.), KI-VO Kommentar, Art. 55, Rn. 9.

56 Art. 55 Abs. 1 lit. b KI-VO.

57 Erwg. 114 KI-VO; so auch Bernsteiner/Schmitt, in: Martini/Wendehorst (Hrsg.), KI-VO Kommentar, Art. 55, Rn. 9.

58 Bernsteiner/Schmitt, in: Martini/Wendehorst (Hrsg.), KI-VO Kommentar, Art. 55, Rn. 9.

59 Art. 55 Abs. 1 lit. c KI-VO.

60 Art. 3 Nr. 49 KI-VO.

Zudem ist ein angemessenes Maß an Cybersicherheit für das KI-Modell und seine physische Infrastruktur zu gewährleisten.[61] Diese Pflicht geht aber nur so weit, wie diese der Anbieter sie auch tatsächlich kontrollieren kann.[62] Die Angemessenheit der Cybersicherheit hängt vom Stand der Technik ab.[63] Hier kann insbesondere mit europäischen und internationalen Normen gearbeitet werden.[64] Weitere Anforderungen an die Cybersicherheit können sich aus der NIS-2-RL[65], dem Cyber Resilience Act[66] und dem Cybersecurity Act[67] ergeben.[68]

## VII. Kollektive KI-Regulierung

Die KI-VO sieht die Möglichkeit der Erstellung sogenannter Praxisleitfäden vor. Diese sollen zur ordnungsgemäßen Anwendung der KI-VO beitragen.[69] Die Anbieter von KI-Modellen und die zuständigen nationalen Behörden erarbeiten, überprüfen und aktualisieren diese Leitfäden.[70] Die Kommission fördert und erleichtert die Ausarbeitung.[71] Organisationen der Zivilgesellschaft, die Industrie, die Wissenschaft und andere einschlägige Interessenträger wie nachgelagerte Anbieter und unabhängige Sachverständige können den Prozess unterstützen.[72] Mittels der Praxisleitfäden sollen die Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, die Einhaltung der KI-VO nachweisen können.[73] Dies gilt allerdings nur so lange, wie keine europäische harmonisierte Norm[74] veröffentlicht worden ist.

## VIII. Durchsetzung der Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

Die Kommission ist primär für die Beaufsichtigung und Durchsetzung der Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck zuständig.[75] Innerhalb der Kommission übernimmt diese Aufgabe das KI-Büro. Dafür erhalten die Kommission und das KI-Büro bestimmte Befugnisse. Darunter fallen allgemeine Überwachungsbefugnisse[76] sowie speziellere

61 Art. 55 Abs. 1 lit. d KI-VO.

62 Bernsteiner/Schmitt, in: Martini/Wendehorst (Hrsg.), KI-VO Kommentar, Art. 55, Rn. 11.

63 Bernsteiner/Schmitt, in: Martini/Wendehorst (Hrsg.), KI-VO Kommentar, Art. 55, Rn. 12.

64 Ebd.

65 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333 S. 80.

66 Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), ABl. L, 2024/2847.

67 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), ABl. L 151 S. 15.

68 Vgl. Bernsteiner/Schmitt, in: Martini/Wendehorst (Hrsg.), KI-VO Kommentar, Art. 55, Rn. 14.

69 Art. 56 Abs. 1 KI-VO.

70 Vgl. Art. 56 Abs. 3 S. 1 KI-VO; Erwg. 116 KI-VO.

71 Art. 56 Abs. 1 KI-VO.

72 Vgl. Art. 56 Abs. 3 S. 2 KI-VO.

73 Art. 53 Abs. 4; Art. 55 Abs. 2 KI-VO.

74 Zur Bedeutung von europäischen harmonisierten Normen siehe: europäische Normen, abrufbar unter: https://europa.eu/youreurope/business/product-requirements/standards/standards-in-europe/index_de.htm.

75 Art. 88 Abs. 1 KI-VO.

76 Art. 89 Abs. 1 KI-VO.

Informationsverlangen.[77] Vor der Übermittlung des Informationsersuchens kann das KI-Büro einen strukturierten Dialog mit dem Anbieter einleiten.[78] Ziel dieses Verfahrens ist die Sondierung der Bereitschaft zur freiwilligen Zusammenarbeit und die Vermeidung von Rechtsstreitigkeiten.[79]

Des Weiteren kann das KI-Büro (nach Konsultation des KI-Gremiums) Bewertungen des betreffenden KI-Modells mit allgemeinem Verwendungszweck durchführen. So kann es die Einhaltung der KI-VO beurteilen, wenn die eingeholten Informationen unzureichend sind.[80] Alternativ kann es eine Bewertung vornehmen, um systemische Risiken auf Unionsebene zu ermitteln.[81] Die Kommission kann über API oder andere geeignete technische Mittel und Instrumente, einschließlich Quellcode, Zugang zu dem betreffenden KI-Modell verlangen.[82] Für die Durchführung von Bewertungen in ihrem Auftrag kann die Kommission unabhängige Sachverständige benennen.[83]

Nachgelagerte Anbieter haben das ausdrückliche Recht, eine Beschwerde wegen eines Verstoßes gegen die KI-VO einzureichen.[84] Diese Beschwerde muss hinreichend begründet sein und inhaltliche Mindestanforderungen erfüllen.[85] So muss etwa eine Beschreibung der einschlägigen Fakten, die betreffenden Bestimmungen der KI-VO und die Begründung des angenommenen Verstoßes enthalten sein.[86]

Neben dem Büro für Künstliche Intelligenz spielt das Gremium für Künstliche Intelligenz eine wichtige Rolle in der Überwachung von KI-Modellen. Das KI-Gremium setzt sich aus einem Vertreter je Mitgliedstaat zusammen.[87] Der Europäische Datenschutzbeauftragte nimmt als Beobachter teil.[88] Andere Behörden oder Stellen der Mitgliedstaaten und der Union oder Sachverständige können im Einzelfall zu den Sitzungen des KI-Gremiums eingeladen werden, wenn die erörterten Fragen für sie von Belang sind.[89] Das Gremium für Künstliche Intelligenz kann dem Büro für Künstliche Intelligenz eine qualifizierte Warnung übermitteln, wenn es Grund zu der Annahme hat, dass ein KI-Modell ein konkretes, identifizierbares Risiko auf Unionsebene birgt.[90] Soweit erforderlich und angemessen, kann die Kommission die Anbieter auffordern, geeignete Maßnahmen zu ergreifen, um ihre Verpflichtungen einzuhalten.[91] Sie hat die Möglichkeit, durch eine entsprechende Anordnung, die Bereitstellung des Modells auf dem Markt zu beschränken, es zurückzunehmen oder zurückzurufen.[92] Bei Verstößen sind Geldbußen für die Anbieter von KI-Modellen mit allgemeinem Verwendungszweck vorgesehen. Diese können bis zu 3 % des gesamten weltweiten Jahresumsatzes eines Unternehmens im vorangegangenen Geschäftsjahr oder 15 000 000 EUR betragen.[93]

---

77 Art. 91 Abs. 1 KI-VO.

78 Art. 91 Abs. 2 KI-VO.

79 Vgl. Bernsteiner/Schmitt, in: Martini/Wendehorst (Hrsg.), KI-VO Kommentar, Art. 92, Rn. 26.

80 Art. 92 Abs. 2 lit. a KI-VO.

81 Art. 92 Abs. 2 lit. b KI-VO.

82 Art. 92 Abs. 3 KI-VO

83 Art. 92 Abs. 2 S. 1 KI-VO.

84 Art. 89 Abs. 2 S. 1 KI-VO.

85 Art. 89 Abs. 2 S. 2 KI-VO.

86 Art. 89 Abs. 2 S. 2 lit. b KI-VO.

87 Art. 65 Abs. 2 S. 1 KI-VO.

88 Art. 65 Abs. 2 S. 2 KI-VO.

89 Art. 65 Abs. 2 S. 4 KI-VO.

90 Art. 90 Abs. 1 lit. a KI-VO.

91 Art. 93 Abs. 1 lit. a KI-VO.

92 Art. 93 Abs. 1 lit. c KI-VO.

93 Art. 101 Abs. 1 KI-VO.

# DFN Infobrief-Recht-Aktuell

## • Verwaltungsrecht/Urheberrecht: Open Innovation und Open Source Strategie des Landes Schleswig-Holstein

Das Land Schleswig-Holstein veröffentlichte im November 2024 seine Open Innovation und Open Source Strategie zu mehr digitaler Souveränität in der Verwaltung. Danach erfolgt in der öffentlichen Verwaltung des Landes ein vollständiger Wechsel flächendeckend auf freie und quelloffene Open-Source-Software. Die „Open Innovation und Open Source Strategie“ strebt den digital souveränen Arbeitsplatz in der Landesverwaltung an.

Hier erhalten Sie den Link dazu:
https://www.schleswig-holstein.de/DE/landesregierung/themen/digitalisierung/linux-plus1

## • Wettbewerbsrecht: Abmahnung durch das Bundeskartellamt (BKartA) gegen Apple

Das BKartA mahnt Apple aufgrund der „App Tracking Transparency Framework“ (ATTF) wegen Verstoßes gegen nationales und europäisches Wettbewerbsrecht ab. Begründet wird dies damit, dass nur Apple selbst im eigenen digitalen Ökosystem personalisierte Werbung anbieten könne. Dadurch missbrauche Apple seine Marktmacht; gleichzeitig müssten Drittanbieter dies als „Tracking“ einstufen.

Hier erhalten Sie den Link zur Pressemitteilung:
https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2025/02_13_2025_Apple_ATTF.html

## • Datenschutzrecht: Stellungnahme des Europäischen Datenschutzausschusses (EDSA) zur Altersverifikation

Der EDSA hat am 11. Februar 2025 eine Stellungnahme zur Altersverifikation angenommen. Altersverifikation umfasst Methoden, um das Alter oder den Altersbereich einer Person zu bestimmen. Die Stellungnahme enthält Leitlinien und Prinzipien aus der Datenschutz-Grundverordnung für die Verarbeitung personenbezogener Daten, die in diesem Kontext den Schutz von Kindern und den Datenschutz in Einklang bringen sollen.

Hier erhalten Sie den Link zur Stellungnahme:
https://www.edpb.europa.eu/system/files/2025-02/edpb_statement_20250211ageassurance_v1-1_en_0.pdf

## • Plattformregulierung: HateAid reicht Beschwerde gegen TikTok bei der Bundesnetzagentur (BNetzA) ein wegen „systemischen Versagens“

Da die Plattform TikTok auf Meldungen rechtswidriger Inhalte wiederholt nicht reagiert hat, reichte die gemeinnützige Organisation HateAid bei der BNetzA eine Beschwerde ein. Sie bezieht sich auf einen mutmaßlichen Verstoß von TikTok gegen Art. 16 Abs. 5 DSA. Danach ist die Plattform verpflichtet, der betreffenden Person unverzüglich seine Entscheidung in Bezug auf gemeldete Informationen mitzuteilen. HateAid geht davon aus, dass TikTok bei zwei Dritteln der eingereichten Beschwerden dieser Verpflichtung nicht nachkommt.

Hier erhalten Sie den Link zur Pressemitteilung:
https://hateaid.org/wp-content/uploads/2025/02/Pressemitteilung-HateAid-Beschwerde.pdf)

# Kurzbeitrag: Ich check das nicht mehr

## Faktenchecks und Communitiy-Notes: Über Grenzen und Anforderungen der Content-Moderation auf sehr großen Online-Plattformen

*von Ole-Christian Tech, Münster*

Spätestens seitdem der Meta Konzern Anfang des Jahres angekündigt hat, künftig zumindest in den USA auf Faktenchecks zu verzichten und stattdessen auf Communitiy-Notes zurückzugreifen, sind die Begriffe Content Moderation, Faktenchecks, Communitiy-Notes und auch der Digital Services Act (DSA) in aller Munde. Befeuert wird die Debatte dabei auch von den Äußerungen des US-amerikanischen Vizepräsidenten J. D. Vance auf der Münchener Sicherheitskonferenz, in welchen er die These aufstellte, die Meinungsäußerungsfreiheit sei in Europa auf dem Rückzug. Um seine These zu untermauern, nutzte er ironischerweise eine Reihe von teilweise irreführenden Ausführungen.[1] Dabei bleibt in der Debatte jedoch oft unklar, was hinter diesen Begriffen steckt und welche rechtliche Relevanz den dahinterstehenden Mechanismen eigentlich zukommt.

## I. Der Zensurvorwurf

Desinformation und Social Media sind oft zwei Seiten derselben Medaille. Die (oft nur vermeintliche) Anonymität in sozialen Medien fördert systemisch unreflektierte, enthemmte und immer häufiger auch aggressive Äußerungen.[2] Gleichzeitig sind Social Media aber auch zunehmend ein Ort der öffentlichen Meinungsbildung und Quelle für Informationen, die oft ähnlich viele Menschen erreichen wie Presse und Rundfunk.[3] Trotz dieser offenkundigen Problematik waren soziale Medien bisher kaum einheitlich reguliert. Mit dem DSA gelten jedoch seit Mitte Februar 2024 europaweit vollständig harmonisierte Regeln für Plattformen wie Facebook, Instagram oder X. Diese verpflichten die sehr großen Online-Plattformen zur Bekämpfung von Desinformation.

Der Chef des Facebook- und Instagram-Mutterkonzerns kritisierte den DSA zuletzt heftig und warf der EU Zensur vor: *"Europe has an ever increasing number of laws institutionalizing censorship and making it difficult to build anything innovative there".*[4]

Anfang 2025 kündigte er an, dass die konzerneigenen Dienste Metas künftig bei der Moderation von Nutzerinhalten auf professionelle Faktenchecks verzichten und stattdessen ein Community-Notes-System einführen werden. X (ehemals Twitter) hatte diesen Schritt bereits im Jahr 2023 vollzogen und die Prüfung von Nutzerinhalten durch Algorithmen oder dazu beauftragte Personen vollständig abgeschafft und stattdessen auf sogenannte Community-Notes gesetzt. Dabei handelt es sich um Kommentare, die andere Nutzer zu einem Beitrag schreiben können, der möglicherweise Falschinformationen enthält. Diese Kommentare werden dann neben dem entsprechenden Tweet angezeigt und sollen diesen in den korrekten Kontext stellen.

1 Steffen/Sanchez Vera, Faktencheck: Behauptungen von Vance zur Meinungsfreiheit, abrufbar unter: https://www.dw.com/de/ist-europas-freiheit-in-gefahr-dsa-digitale-dienste-unterdr%C3%BCckung/a-71660852

2 Wagner, ZUM 2022, 861 (863).

3 Wagner, ZUM 2022, 861 (861).

4 Wax/Haeck, Zuckerberg's censorship claims were 'misleading' — EU tech chief, https://www.politico.eu/article/mark-zuckerberg-meta-misleading-censorship-henna-virkkunen/.

Diese sogenannten Notes werden zunächst auf einer eigenen, von der Hauptplattform getrennten Plattform, dem sogenannten Backend, veröffentlicht. Hier können die Notes dann von den Nutzern bewertet werden. Sofern ein Kommentar genügend Bewertungen erhält, wird er auch auf der Hauptplattform angezeigt.[5] Damit soll die freie Meinungsäußerung gefördert werden.

## II. Der DSA und seine Rolle im Kampf gegen Desinformation

Der Fokus der Bestimmungen des DSA liegt auf dem Bestreben, digitale Plattformen vertrauenswürdiger und sicherer zu machen. Zur Verwirklichung dieser Ziele setzt die EU auf die Eindämmung gesetzeswidriger Online-Aktivitäten. Ein zentraler Aspekt des Regelwerks ist dabei die Definition von „rechtswidrigen Inhalten", die jegliche Verstöße gegen europäisches oder nationales Recht umfasst, vgl. Art. 3 lit. h DSA. In der Praxis kann dies von Urheberrechtsverletzungen bis hin zu Ehrdelikten (z. B. Beleidigung gem. § 185 StGB oder Verleumdung gem. § 187 StGB) oder Staatsschutzdelikten (z. B. Verbreiten von Propagandamitteln verfassungswidriger und terroristischer Organisationen gem. § 86 StGB) eine erhebliche Bandbreite an Inhalten betreffen. Gerade nicht per se rechtswidrig sind hingegen Desinformationen, sogenannte Fake News. Vielmehr sind solche Äußerungen oftmals rechtmäßig und wegen der Vermischung von Tatsachenbehauptungen und Werturteilen sogar meist von der Meinungsfreiheit gedeckt.[6] Greift der DSA in diesem Punkt also womöglich zu kurz?

Die Problematik der Desinformation auf digitalen Plattformen wurde in der Vergangenheit wiederholt evident, insbesondere während der Covid-19-Pandemie, als fragwürdige Gesundheitshinweise in sozialen Netzwerken Hochkonjunktur hatten und eine Gefährdung der öffentlichen Ordnung und Gesundheit darstellten. Ebenfalls stellte sich das Problem in gravierendem Maße nach Beginn der Kriege in der Ukraine und im Nahen Osten. Mit Blick darauf findet sich in Art. 34 Abs. 1 DSA die Verpflichtung für die Anbieter sehr großer Online-Plattformen, alle systemischen Risiken in der Union, die aus der Konzeption oder dem Betrieb ihrer Dienste resultieren, sorgfältig zu ermitteln, zu analysieren und zu bewerten. Dies erfasst nach Art. 34 Abs. 1 lit. c DSA auch „alle tatsächlichen oder absehbaren nachteiligen Auswirkungen auf die gesellschaftliche Debatte und auf Wahlprozesse und die öffentliche Sicherheit." An diese Pflicht zur Risikobewertung knüpft die in Art. 35 Abs. 1 DSA normierte Pflicht zur Risikominderung an.[7] Die EU zielt mit dieser Maßnahme insbesondere auf die Verringerung der potenziellen gesellschaftlichen Risiken ab, die mit der Verbreitung von Desinformation oder anderen Inhalten einhergehen können.[8] Für sehr große Online-Plattformen (Art. 33 Abs. 1 DSG) besteht demnach ein signifikantes Haftungsrisiko. Im Falle von Zuwiderhandlungen gegen die auferlegten Sorgfaltspflichten, wie beispielsweise die Pflicht zur Bekämpfung von Desinformation oder die Minderung von Systemrisiken für die gesellschaftliche Debatte (Art. 35 Abs. 1, 34 Abs. 1 UAbs. 2 lit. c DSA) können Bußgelder in Höhe von bis zu 6 % des im Vorjahr weltweit erzielten Konzernumsatzes verhängt werden (vgl. Art. 52 DSA).[9] Desinformationen werden somit zwar nicht explizit in den Vorschriften des DSA genannt, jedoch trotzdem geahndet. Die Maßnahmen zur Risikominderung müssen dabei angemessen, verhältnismäßig und wirksam sein, eine Pflicht zur Anwendung bestimmter Maßnahmen existiert nicht. Beispielhaft führt Art. 35 Abs. 1 lit. c DSA etwa die „Anpassung der Verfahren zur Moderation von Inhalten" auf.[10]

Zur Erfüllung dieser Pflichten haben die Plattformen zuletzt auf eine Content Moderation gesetzt, die auch eine Kooperation mit professionellen Faktencheckern beinhaltete. Diese Faktenchecker können bei den Plattformen selbst rechtswidrige bzw. strafbare

5 Die Einordnung einer Community-Note unterliegt einem ausdifferenzierten Prozess und erfolgt nicht lediglich nach dem Mehrheitsprinzip. Für eine anschauliche Darstellung vgl. Bovermann, Community Notes auf dem Prüfstand, VerfBlog, abrufbar unter: https://verfassungsblog.de/community-notes-auf-dem-prufstand/.

6 Kastor/Püschel, K&R 2023, 20 (20) m.w.N.

7 Aus Erwägungsgrund 104 zum DSA lässt sich schließen, dass auch Fake News zu den systemischen Risiken zählen können.

8 Erwägungsgrund Nr. 9 S. 1 zum DSA.

9 Bovermann, Community Notes auf dem Prüfstand, VerfBlog, abrufbar unter: https://verfassungsblog.de/community-notes-auf-dem-prufstand/.

10 Umfassend zur Geeignetheit des Fact Checkings als Risikominderungsmaßnahme: Kastor/Püschel, K&R 2023, 20 (20) m.w.N.

Inhalte (z. B. beleidigende Äußerungen, s. o.), aber auch Fake News melden.[11] Die Plattformen sind verpflichtet, diese Meldungen vorrangig zu behandeln und unverzüglich zu bearbeiten.

Rein rechtlich erscheint es aber möglich, dass eine Plattform die Zusammenarbeit mit den Faktencheckern aufkündigt und durch besagte Community-Notes ersetzt, sofern diese wirksam sind.

## III. Fazit und Relevanz für wissenschaftliche Einrichtungen und Hochschulen

Im Ergebnis spielt die konkrete Art der Content-Moderation also keine entscheidende Rolle, der DSA schreibt gerade kein bestimmtes Verfahren vor. Entscheidend ist vielmehr die Effektivität der implementierten Maßnahmen zur Mitigation systemischer Risiken. Um sich vor einer Haftung für rechtswidrige Inhalte zu schützen, stehen Plattformen vor dem Dilemma, entweder zu viel zu blockieren und damit die Meinungsäußerungsfreiheit zu verkürzen oder zu wenig einzugreifen und damit zu haften. Faktenchecker übernehmen an dieser Stelle zum einen die Identifizierung problematischer Inhalte, zum anderen können sich die Plattformen bei möglichen Fehlern sogar exkulpieren.[12] Auch ist die Wirksamkeit von Community-Notes allein nicht unbestritten.[13] Diese sind z. B. potenziellen Manipulationen durch Nutzer ausgesetzt, die etwa durch Absprachen die Sichtbarkeit der Community-Notes beeinflussen oder dafür sorgen können, dass ein Fokus auf bestimmte Inhalte entsteht. Die zukünftige Entwicklung wird zeigen, ob große Plattformen tatsächlich auf dieses Instrument zurückgreifen wollen und welche Haftungsrisiken sich realisieren.

Auch wissenschaftliche Einrichtungen und Hochschulen sind im Rahmen ihrer Öffentlichkeitsarbeit vielfach auf digitalen Plattformen vertreten, oftmals auch auf jenen, die zunehmend weniger moderiert werden. In jüngster Zeit verlassen jedoch immer mehr Einrichtungen und Wissenschaftler bestimmte Plattformen.[14] Empfehlungen für einen angemessenen Umgang mit diesen Plattformen sind nur bedingt möglich, jedoch sollte berücksichtigt werden, dass wissenschaftliche Einrichtungen und Hochschulen durch ihre Öffentlichkeitsarbeit die Möglichkeit haben, durch die Publikation von Forschungsergebnissen und die transparente Erklärung wissenschaftlicher Prozesse, Desinformationen entgegenzuwirken. Ein etwaiger Rückzug aus diesen digitalen Räumen ist daher auch aus diesem Blickwinkel zu beobachten.

---

11 Hierzu vertiefend auch Hentsch, Könnte Meta auf Faktenchecks verzichten?, https://www.lto.de/recht/hintergruende/h/ankuendigung-mark-zuckerberg-abschaffung-faktenchecks-facebook-instagram-rechtslage-europa-dsa.

12 Hentsch, Könnte Meta auf Faktenchecks verzichten?, abrufbar unter https://www.lto.de/recht/hintergruende/h/ankuendigung-mark-zuckerberg-abschaffung-faktenchecks-facebook-instagram-rechtslage-europa-dsa.

13 Vgl. dazu Brunner/Kafsack/Sachse, Fußnoten gegen Faktenprüfer, Frankfurter Allgemeine Zeitung vom 10.01.2025, S. 25.

14 Unis und Social Media: 60 Hochschulen verlassen X, https://www.faz.net/aktuell/feuilleton/sechzig-hochschulen-verlassen-x-gegen-rechtspopulistische-botschaften-110228028.html.

## 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 Freien 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

Freie Universität Berlin
Professur für Bürgerliches Recht,
Wirtschafts-, Wettbewerbs- und
Immaterialgüterrecht
Prof. Dr. Katharina de la Durantaye, LL. M. (Yale)
Van't-Hoff-Str. 8, 14195 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