„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

8 / 2025
August 2025

Lex Data

Ideen für ein allgemeines Datengesetzbuch

KI-Kompetente Hochschulen

Hochschulen müssen sicherstellen, dass ihre Mitarbeiter:innen über KI-Kompetenz verfügen, wenn sie KI einsetzen

Urteile für alle

Zur Haftung der freien Rechtsprechungsdatenbank openJur für einen Datenschutzverstoß

Kurzbeitrag: Rote Karte für den Betriebsratsvorsitzenden

Weiterleitung sensibler Personaldaten an private E-Mail-Adresse als grobe Pflichtverletzung

Lex Data

Ideen für ein allgemeines Datengesetzbuch

Von Anna Maria Yang-Jacobi, Münster

In den letzten Jahren wurden sowohl auf europäischer als auch auf nationaler Ebene viele Gesetze verabschiedet, die den Umgang mit Daten betreffen. Beispielhaft seien die Free-Flow-of-Data-Verordnung, der Data Governance Act, der Data Act oder das Datennutzungsgesetz genannt. Die Menge an gesetzlichen Vorgaben nimmt dabei stetig zu und berührt regelmäßig nur spezifische Bereiche. Im Koalitionsvertrag von CDU, CSU und SPD[1] gibt es Pläne für mehr Einheitlichkeit. So bestehen Überlegungen, die „Datengesetze" noch in dieser Legislaturperiode in einem allgemeinen Datengesetzbuch zu bündeln.

I. Bisherige „Gesetze mit Datenbezug"

Daten sind in aller Munde. Dabei existieren je nach Wissenschaftsbereich verschiedene Definitionen von Daten. Grundsätzlich handelt es sich um die digitale Abbildung von Handlungen, Tatsachen oder Informationen.[2] Nachdem es viele Jahre in der Gesetzgebung vor allem um den Schutz von personenbezogenen Daten gegangen war, hat sich der Fokus mittlerweile gewandelt. In jüngster Zeit wird die Nutzung von Daten, zum Beispiel in der Industrie bzw. zu statistischen Zwecken oder beim Training Künstlicher Intelligenz,[3] vermehrt diskutiert. Dabei rückt die wirtschaftliche Bedeutung von Daten ins Zentrum der Diskussionen, sodass auch über Möglichkeiten des Datenteilens beraten wird. Die Europäische Kommission hat bereits 2020 eine umfangreiche Datenstrategie[4] verabschiedet. Die Ampelregierung hatte ihrerseits für die vergangene Legislaturperiode Gesetze mit Bezug auf Daten geplant. Diese Gesetzesvorhaben werden zum Teil von der schwarz-roten Bundesregierung wieder aufgegriffen.

1. Europäische Rechtsakte

Auf europäischer Ebene existiert eine Vielzahl von Rechtsakten, die sich auf Daten beziehen. Bereits vor fast 25 Jahren entstand ein eEurope 2002 Aktionsplan[5]. Damals ging es noch hauptsächlich darum, den Internetzugang in Europa zu verbreiten und zu fördern. Allerdings enthielt selbst dieser Aktionsplan erste Überlegungen zur Datennutzung.

In der Zwischenzeit wurden einige der EU-Rechtsakte aus dieser Zeit ersetzt oder zumindest reformiert. So beispielsweise die e-Privacy-Richtlinie[6] von 2002, die verbindliche Mindestvorgaben

1 Koalitionsvertrag, 21. Legislaturperiode 2025-2029, https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf (alle Links dieses Beitrags wurden zuletzt am 7.7.2025 abgerufen).

2 So beispielsweise die Definition in Art. 2 Nr. 1 Data Governance Act sowie Art. 2 Nr. 1 Data Act.

3 In diesem Fall geht es trotz des Kontexts der Nutzung daneben weiterhin um den Schutz personenbezogener Daten. Die Datenschutzkonferenz (DSK) hatte bereits 2024 eine Orientierungshilfe herausgegeben, siehe dazu Müller, Künstliche Intelligenz – keine Innovation ohne Diskretion?, DFN-Infobrief Recht 9/2024.

4 EU-Kommission, COM(2020) 66 final, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020DC0066.

5 https://eur-lex.europa.eu/DE/legal-content/summary/eeurope-2002.html.

6 Richtlinie 2002/58/EG des Europäischen Parlaments und des Dates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

für den Datenschutz in der Telekommunikation enthält. 2009 kamen insbesondere Regelungen zur Speicherung und Nutzung von Daten auf Nutzerendgeräten hinzu. Als EU-Richtlinie musste eine Umsetzung in das nationale Recht der Mitgliedstaaten erfolgen, Art. 288 Abs. 3 AEUV. In Deutschland sind die Vorgaben, nach Stationen im Telekommunikationsgesetz (TKG) und im Gesetz gegen den unlauteren Wettbewerb (UWG), (und teilweise mit einiger Verspätung) im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) umgesetzt worden.[7]

Außerdem existiert bereits seit 2003 die Open Data-Richtlinie (auch PSI-RL genannt).[8] 2013 und 2019 erfolgten umfassende Überarbeitungen der PSI-RL, die ebenfalls in nationales Recht umgesetzt werden mussten. Die Richtlinie fördert die Offenlegung und Nutzung öffentlich zugänglicher Daten öffentlicher Stellen.[9] Dabei handelt es sich um Daten wie Informationen über die Umwelt, das Wetter, den Verkehr, die Gesundheit, Finanzen und andere Bereiche des öffentlichen Interesses, die öffentliche Stellen im Rahmen ihrer Aufgaben sammeln und verwalten. Ziel ist es, den Zugang zu diesen Daten zu erleichtern und deren Wiederverwendung zu fördern. So sollen wettbewerbliche Nachteile europäischer Unternehmen ausgeglichen werden. Entsprechend werden die öffentlichen Stellen zu einer Bereitstellung dieser Daten verpflichtet. In Deutschland findet sich die Umsetzung im Datennutzungsgesetz.

2016 folgte die Datenschutzgrundverordnung (DSGVO).[10] Sie zielt darauf ab, die Regeln zur Verarbeitung personenbezogener Daten durch Verantwortliche europaweit zu vereinheitlichen. Der Schutz personenbezogener Daten innerhalb der EU, aber auch der freie Datenverkehr im EU-Binnenmarkt, soll gewährleistet werden, Art. 1 Abs. 1 DSGVO. Neben der DSGVO wurde 2016 auch eine EU-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden und Strafvollstreckung (JI-RL)[11] verabschiedet, die in Deutschland im Bundesdatenschutzgesetz (BDSG) umgesetzt wurde.

Nach diesen Regelungen zum Schutz personenbezogener Daten verabschiedete der EU-Gesetzgeber ergänzend Ende 2018 mit der Free-Flow-of-Data-Verordnung (auch bekannt als Datenverkehrs-VO)[12], eine spezielle Verordnung, die den freien Verkehr nicht personenbezogener Daten betrifft.[13] Innerhalb der EU sollte auch in diesem Bereich ein freier, digitaler Binnenmarkt gestärkt werden. So ist es über die Free-Flow-of-Data-VO für Unternehmen und die öffentliche Verwaltung möglich, nicht personenbezogene Daten überall in der EU zu speichern, zu übertragen und zu verarbeiten. Bisherige Datenlokalisierungsauflagen nach dem jeweiligen nationalen Recht der Mitgliedstaaten, die eine Übertragung ins EU-Ausland untersagten, gehören somit der Vergangenheit an. Der Zugriff von Behörden auf die im Ausland gespeicherten Daten muss jedoch gewährleistet sein.

Die darauffolgende europäische Datenstrategie von 2020 ist Teil einer noch weiter angelegten Digitalstrategie der EU-Kommission.[14] Im Rahmen der Digitalstrategie sind auch der Digital Services Act (DSA) und der Digital Markets Act (DMA) von Bedeutung, die

---

7 Zum TDDDG siehe nur, John, Ein Tool, die Banner zu knechten, DFN-Infobrief Recht 1/2022 sowie Yang-Jacobi, Telemedien out, Digitale Dienste in!, DFN-Infobrief Recht 8/2024.

8 Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors.

9 Zur derzeitigen Fassung siehe genauer Tech, Datenstaat oder Datensalat?, DFN-Infobrief Recht 8/2023.

10 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

11 Richtlinie (EU) 2016/680 des Europäisches Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen und bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

12 Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union.

13 Siehe auch Tech, Datenstaat oder Datensalat?, DFN-Infobrief Recht 8/2023.

14 EU-Kommission, C(2022) 4388 final, 30.6.2022, https://commission.europa.eu/document/download/1ffd42a0-2a49-447b-b084-87ef9996ad13_de?filename=C_2022_4388_1_DE_ACT.

spezifische Datenzugangsansprüche enthalten.[15] Im Rahmen der europäischen Datenstrategie wurden und werden nochmals eine Reihe von Rechtsakten nach und nach verabschiedet. Die Datenstrategie hat zum Ziel, die branchenübergreifende Nutzung von Daten zu fördern, wobei gleichzeitig Datenschutzstandards und Verbraucherrechte gewahrt werden sollen. Zur Datenstrategie gehören der Data Governance Act, der Data Act sowie die weitgehend zukünftigen Regelungen zu Datenräumen.

Der Data Governance Act gilt seit September 2023 und soll den Datenaustausch zwischen öffentlichen Sektoren und Mitgliedstaaten der EU fördern. Dabei werden Verhaltenspflichten für Datenvermittlungsdienste und datenaltruistische Organisationen festgelegt. Zudem verabschiedete der EU-Gesetzgeber Ende 2023 den Data Act.[16] Dieser trifft Regelungen zur fairen Nutzung und dem Zugang zu personenbezogenen und nicht personenbezogenen Daten, die bei der Verwendung von Produkten und Diensten anfallen. Daten sollen Wirtschaftsteilnehmenden als wirtschaftliches Gut leichter zugänglich gemacht werden. So ergeben sich Pflichten zur Zugänglichmachung und Bereitstellung von Daten, zur Weitergabe oder auch zur Bereitstellung gegenüber öffentlichen Stellen. Die Bestimmungen des Data Acts zu den verbundenen Produkten gelten ab September 2025. Zusätzlich werden nach und nach sektorspezifische EU-Regelungen zu gemeinsamen Datenräumen geschaffen.[17] Im März 2025 ist die Verordnung über einen Europäischen Gesundheitsdatenraum (EDHS-VO)[18] als erster sektorspezifischer Datenrechtsakt in Kraft getreten. Sie schafft einen gemeinsamen Rahmen für die Nutzung und den Austausch elektronischer Gesundheitsdaten in der EU. Die Regelungen finden jedoch erst schrittweise Anwendung (frühstens ab März 2027, teilweise auch erst ab März 2031). Weitere sektorspezifische Regelungen sollen folgen, wie zum Beispiel im Automobilbereich, in der Landwirtschaft sowie im Bereich Forschung und Innovation.

All diese Rechtsakte mit Bezug auf Daten enthalten Elemente unterschiedlicher Rechtsgebiete und bilden die Grundlage für ein (vergleichsweise) neues Rechtsgebiet: das Datenrecht. Dieses Rechtsgebiet befindet sich im ständigen Wandel. Allgemein werden dem Datenrecht bisher sowohl Rechtsakte zu personenbezogenen als auch zu nicht personenbezogenen Daten zugeordnet. Als übergeordnetes Prinzip kann die Regulierung der Generierung, Nutzung, Auswertung und Weitergabe von Daten festgestellt werden.

2. Nationale Gesetze

Auf nationaler Ebene sind zunächst die Umsetzungsgesetze der europäischen Richtlinien zu nennen, also das TDDDG, Teile des BDSG und insbesondere auch das Datennutzungsgesetz. Hinzu kommen Durchführungsgesetze, welche die Zuständigkeiten und Sanktionen von EU-Verordnungen für die nationale Durchführung festlegen. Die Entwürfe zu den Durchführungsgesetzen des Data Governance Act[19] und Data Acts[20] liegen bereits vor, müssen jedoch noch vom Bundestag verabschiedet werden.

Die Ampelregierung sah in der vergangenen Legislaturperiode im „Datenbereich“ den Erlass von Gesetzen wie dem Gesundheitsdatennutzungsgesetz (GDNG), dem Mobilitätsdatengesetz, dem Forschungsdatengesetz, eine Reform des BDSG und ein Beschäftigtendatengesetz vor.[21] Das GDNG trat im März 2024 in Kraft und ermöglicht die Nutzung von Gesundheitsdaten zu Forschungszwecken und einer datenbasierten Weiterentwicklung des

15 Zum DSA siehe v. Bernuth, Die fabelhafte Welt der digitalen Dienste, DFN-Infobrief Recht 7/2025; v. Bernuth, Datenzugangsrechte im DSA, DFN-Infobrief Recht 3/2025; v. Bernuth, Systemische Risiken riesiger Systeme, DFN-Infobrief Recht 9/2024 sowie zum DMA siehe Yang-Jacobi, Google im Visier der Behörden und Gerichte, DFN-Infobrief Recht 1/2025; Rennert, Brüssel reguliert das schon, DFN-Infobrief Recht 6/2022.

16 Dazu auch Müller, Die Daten sind frei?, DFN-Infobrief Recht 3/2024; Schaller, Data Act: Mehr Daten für alle – check!, DFN-Infobrief Recht 6/2022.

17 Zum aktuellen Stand siehe die Übersicht der EU-Kommission, https://digital-strategy.ec.europa.eu/de/policies/data-spaces.

18 Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847.

19 Die EU-Kommission hat gegen Deutschland bereits ein Vertragsverletzungsverfahren bezüglich der Durchführung des Data Governance Acts eingeleitet.

20 Dazu Geiselmann, Kurzbeitrag: Von Netz zu Netz, DFN-Infobrief Recht 5/2025.

21 Koalitionsvertrag, 20. Legislaturperiode 2021-2025, S. 14, 18, 41, 65, https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf

Gesundheitswesens, § 1 Abs. 1, 2 GDNG. Die anderen genannten Vorhaben scheiterten allerdings am Bruch der Ampelkoalition.[22] Die aktuelle Bundesregierung legt jedoch auch einen Fokus auf den Datenbereich. Es soll eine Kultur der Datennutzung und des Datenteilens entstehen. Eine Datenwirtschaft soll etabliert werden, wobei auch der Schutz von Grund- und Freiheitsrechten elementar sein soll. Bisher wurden aber noch keine neuen Entwurfsversionen der anvisierten Gesetzesvorhaben veröffentlicht.

II. Wie könnte ein allgemeines Datengesetzbuch aussehen?

Allein diese Aufzählung der Rechtsakte auf EU- und nationaler Ebene zeigt: Das Datenrecht besteht aus vielen einzelnen Rechtsakten. Die schiere Anzahl an Regelungen macht es schwer, den Überblick zu behalten. Eine Zersplitterung des Rechts droht - gerade, weil voraussichtlich in Zukunft viele weitere „Gesetze mit Datenbezug" nebeneinander verabschiedet werden.

Die Lösung für etwas mehr Rechtsklarheit und Einheitlichkeit – zumindest im nationalen Recht – könnte ein allgemeines Datengesetzbuch darstellen. Auf EU-Ebene könnten zwar auch Veränderungen hingehend zu einheitlichen „Omnibus"-Rechtsakten zur Sammlung der einzelnen Rechtsakte diskutiert werden (jüngst wurden Omnibus-Pakete zu Vorschriften für Nachhaltigkeitsberichterstattung und EU-Investitionen verabschiedet), aber bislang liegen keine konkreten Pläne vor. Gerade weil die EU-Rechtsakte allerdings teilweise verbindliche Regelungen vorsehen, müsste ein nationales allgemeines Datengesetzbuch einen Ergänzungs- und Kooperationscharakter aufweisen und modular ergänzt werden können. Die Bundesregierung hat diese Überlegung bereits im Koalitionsvertrag für die verschiedenen Regelwerke zur Nutzung und zum Teilen von Daten vorgesehen.[23] Die Vorteile eines allgemeinen Datengesetzbuchs liegen dabei auf der Hand: Das Datenrecht würde nicht weiter fragmentieren, bestehende und künftige Vorhaben könnten gebündelt und mögliche Reibungen zwischen den einzelnen Rechtsakten gelöst werden. Konkrete Entwürfe für ein allgemeines Datengesetzbuch gibt es bislang aber noch nicht.

Das Vorhaben wurde jedoch bereits von Rechtswissenschaftler:innen aufgegriffen und bewertet, um die Debatte in diese Richtung zu eröffnen.[24] Dabei stellten sie fest, dass es unterschiedliche Optionen für ein allgemeines Datengesetzbuch gibt. Einerseits könnte man verschiedene bereits existierende und künftig zu erwartende Regelwerke in einem Gesetzbuch zusammenführen, also im Grunde redaktionell zusammenfassen. Andererseits wäre auch eine ambitioniertere, systematisch gliedernde Kodifikation datenbezogener Rechtsfragen möglich. Genauer könnten die bestehenden und geplanten nationalen Regulierungsvorhaben darin gebündelt werden. Zusätzlich wäre es auch möglich, weitere Rechtsmaterien einzubinden, die traditionell national geregelt werden oder außerhalb des Anwendungsbereichs der EU liegen. Das sind beispielsweise das Vertragsrecht oder die nationale Sicherheit. Zu den geplanten nationalen datenrechtlichen Gesetzen könnten Regelungen zur Anreizsetzung hinzukommen, etwa zugunsten des Datenaltruismus oder datenaltruistischer Organisationen.[25] Des Weiteren könnten sich auch Regelungen zur privaten Rechtsdurchsetzung im Datenrecht, zum Datenvertragsrecht inkl. zu den Allgemeinen Geschäftsbedingungen im Bereich des Vertragsrechts mit Verbraucher:innen sowie auch zu Datenzugangsregelungen im Verteidigungsfall bzw. Zivilschutz anschließen. Gerade in den Bereichen Verteidigung und Zivilschutz gibt es nur punktuelle gesetzliche Regelungen, die teilweise bereits etwas veraltet sind. Diese nationalen Bestimmungen könnten ergänzend zu den Datenzugangsansprüchen von öffentlichen Stellen bei außergewöhnlicher Notwendigkeit nach Art. 14 ff. Data Act erlassen werden.

Die datenrechtlichen Themen wurden in der Diskussionsgrundlage sodann bereits gegliedert. Das Datengesetzbuch könnte dabei aus fünf größeren Abschnitten bestehen: einem allgemeinen Teil, dem Datenprivatrecht, dem Datenaußenwirtschaftsrecht, den sektorspezifischen Regelungen sowie der Rechtsdurchsetzung.

---

22 https://netzpolitik.org/2025/netzpolitische-bilanz-welche-ihrer-ziele-hat-die-ampel-erreicht-und-welche-nicht/; https://www.heise.de/hintergrund/Auslegungssache-128-Scherbenhaufen-Beschaeftigtendatenschutz-10289273.html.

23 Koalitionsvertrag, 21. Legislaturperiode 2025-2029, S. 69, https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf.

24 Allen voran Hennemann/Wendehorst, 15.4.2025, S. 3, https://uni-freiburg.de/jura-medienrecht/wp-content/uploads/sites/34/74b487873ff2942cde10b53a3791f76ce3e22f07a6e16ce9c924b9a14558.pdf, deren Überlegungen im Folgenden dargestellt werden.

25 Im Data Governance Act sind bisher nur Verpflichtungen geregelt.

Der allgemeine Teil enthält das Datenkollisionsrecht, behandelt also die Frage, welches Recht bei grenzüberschreitenden Rechtsstreitigkeiten anzuwenden ist. Zudem umfasst er die Definitionen bedeutsamer Begriffe, Regelungen zu Datenformaten, Datenstandards und Registern sowie Maßnahmen zur Förderung der Datenkompetenz. Das Datenprivatrecht befasst sich als nächster großer Abschnitt vor allem mit dem Datenvertragsrecht und ggf. auch mit einem Datenhandelsrecht. Im Datenaußenwirtschaftsrecht können Verpflichtungen zum Datenzugang im privaten Sektor, bei Open Data (also frei zugängliche und damit frei weiterverwendbare Daten) und im öffentlichen Sektor ihren Platz finden sowie Regelungen zur Datensicherung, Datenlokalisation oder zum Datenaußenwirtschaftsrecht. Die sektorspezifischen Regelungen würden die Vorgaben zu Mobilitätsdaten, Forschungsdaten, Gesundheitsdaten, Geodaten, Geologiedaten und weitere Daten enthalten. Im finalen Abschnitt könnte die Rechtsdurchsetzung in eine private (also die Durchsetzung rechtlicher Vorgaben durch Private im Rahmen von Zivilprozessen, beispielsweise über private Schadensersatzklagen) und eine behördliche Rechtsdurchsetzung durch (Aufsichts-)Behörden aufgeteilt werden. Im behördlichen Bereich wären vor allem die Regelungen der Durchführungsgesetze enthalten.

Selbstverständlich sind dies nur erste Überlegungen und sollen lediglich den Anstoß zu weiteren rechtswissenschaftlichen Diskussionen liefern. Rechtsanwender:innen würde es jedoch bereits sehr helfen, die einzelnen Rechtsakte mit Datenbezug redaktionell gebündelt vorzufinden. Im Sinne einer Vereinfachung des Rechts wäre ein allgemeines Datengesetzbuch definitiv zu begrüßen.

III. Bedeutung für Hochschulen und Forschungseinrichtungen

Ob und bis wann ein allgemeines Datengesetzbuch tatsächlich kommt, wird die Zukunft zeigen. Für Hochschulen und Forschungseinrichtungen sind die Überlegungen zu einem allgemeinen Datengesetzbuch vor allem im Hinblick auf den Datenzugang im öffentlichen Sektor interessant. Aber auch allgemeine Regelungen zu Datenformaten, Datenstandards und Maßnahmen zur Förderung der Datenkompetenz wären für die Rechtsanwendung hilfreich. Daneben sind selbstverständlich die sektorspezifischen Regelungen zu Forschungsdaten von besonderer Bedeutung.

So wäre für Hochschulen und Forschungseinrichtungen zu hoffen, dass das Forschungsdatengesetz[26] schon bald Realität wird. Forschungseinrichtungen wie das Deutsche Institut für Wirtschaftsforschung haben bereits gefordert, das Forschungsdatengesetz zu priorisieren. Der Zugang zu Forschungsdaten müsse verbessert werden. Immerhin führe eine größere Datenverfügbarkeit auch zu mehr wissenschaftlichen Veröffentlichungen, und wissenschaftliche Ergebnisse würden vermehrt in politische Entscheidungsprozesse eingebunden werden.[27] Das Bundesministerium für Bildung und Forschung (BMBF) hatte bereits 2024 (noch unter der Leitung der Ampel-Koalition) Eckpunkte für ein Forschungsdatengesetz[28] vorgestellt. Zuvor fand eine Konsultation der Wissenschaftslandschaft statt. Ziel des Forschungsdatengesetzes wäre demnach, einen zentralen Rahmen für den Zugang zu Forschungsdaten zu schaffen. Allen voran soll es die rechtlichen Grundlagen für eine Datentreuhandstelle (sogenanntes Micro Data Center) schaffen sowie den Zugang zu Daten der öffentlichen Hand verbessern. Dafür soll das Forschungsdatengesetz auch gesetzliche Zugangsansprüche für Forschungseinrichtungen und Hochschulen enthalten. Zudem sind Anpassungen im Datenschutzrecht zugunsten der Forschung sowie die Einführung von Metadatenkatalogen vorgesehen. Sofern der Gesetzesentwurf der neuen Bundesregierung auf den Überlegungen des bereits bekannten Eckpunktepapiers aufbaut, sollen die Regelungen sowohl für öffentliche als auch private Forschungseinrichtungen und Hochschulen gelten. Der konkrete Gesetzesentwurf soll zum Jahresende 2025 folgen.[29] Wahrscheinlich – und wenn überhaupt – werden sich erst danach Überlegungen zu einem allgemeinen Datengesetzbuch konkretisieren.

---

26 Dazu auch v. Bernuth, Alte Bekannte und etwas Neuland, DFN-Infobrief Recht 5/2025.

27 Schiersch/Ullrich, DIW aktuell, 21.3.2025, S. 3, https://www.diw.de/documents/publikationen/73/diw_01.c.942112.de/diw_aktuell_115.pdf.

28 BMBF, Eckpunkte Forschungsdatengesetz, 28.2.2024, https://www.bmbf.de/SharedDocs/Downloads/DE/gesetze/forschungsdatengesetz/sonstige/Eckpunktepapier.pdf?__blob=publicationFile&v=3.

29 Koalitionsvertrag, 21. Legislaturperiode 2025-2029, S. 79, https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf.

KI-Kompetente Hochschulen

Hochschulen müssen sicherstellen, dass ihre Mitarbeiter:innen über KI-Kompetenz verfügen, wenn sie KI einsetzen

Von Philipp Schöbel, Berlin

Seit dem 2. Februar 2025 gilt die Pflicht zur KI-Kompetenz. Danach müssen Anbieter und Betreiber von KI-Systemen unabhängig von deren Risikograd sicherstellen, dass nach besten Kräften ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen.[1] Diese betrifft auch Hochschulen – unabhängig ob staatlich oder privat. Die behördliche Kontrolle dieser Pflicht wird voraussichtlich ab dem 3. August 2026 erfolgen. Die Europäische Kommission hat inzwischen FAQ zur KI-Kompetenz veröffentlicht.[2] Zeit, sich mit dem Inhalt der Pflicht genauer auseinanderzusetzen.

I. KI-Kompetenz im Sinne der KI-VO

Die KI-Verordnung (KI-VO)[3] definiert KI-Kompetenz als „die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden."[4] Anbieter und Betreiber von KI-Systemen müssen sicherstellen, dass die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasste Personen, „über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind."[5]

Erwägungsgrund Nr. 20 der KI-VO trifft weitere Aussagen zur KI-Kompetenz. Die KI-Kompetenz sollte demnach Anbieter, Betreiber und betroffene Personen mit den notwendigen Konzepten ausstatten, um fundierte Entscheidungen über KI-Systeme zu treffen. So sollen der größtmögliche Nutzen aus KI-Systemen gezogen und gleichzeitig die Grundrechte, Gesundheit und Sicherheit gewahrt sowieeine demokratische Kontrolle ermöglicht werden. Diese notwendigen Konzepte könnten in Bezug auf den jeweiligen Kontext variieren. Dies könne das Verstehen der korrekten Anwendung technischer Elemente in der Entwicklungsphase des KI-Systems, der bei seiner Verwendung anzuwendenden Maßnahmen und der geeigneten Auslegung der Ausgaben des KI-Systems umfassen. Für betroffene Personen könne dies weiterhin auch das nötige Wissen umfassen, um zu verstehen, wie sich mithilfe von KI getroffene Entscheidungen auf sie auswirken werden. Die KI-Kompetenz soll allen einschlägigen Akteuren entlang der KI-Wertschöpfungskette die Kenntnisse vermitteln,

1 Art. 4 KI-VO.

2 Europäische Kommission, AI Literacy - Questions & Answers, 07.05.2025, abrufbar unter: https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers (alle Links zuletzt abgerufen am 03.07.2025).

3 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. L, 2024/1689, 12.7.2024.

4 Art. 3 Nr. 56 KI-VO.

5 Art. 4 KI-VO.

die erforderlich sind, um die angemessene Einhaltung und die ordnungsgemäße Durchsetzung der Verordnung sicherzustellen. Die umfassende Umsetzung von KI-Kompetenzmaßnahmen und die Einführung geeigneter Folgemaßnahmen könnten dazu beitragen, die Arbeitsbedingungen zu verbessern und letztlich die Konsolidierung und den Innovationspfad vertrauenswürdiger KI in der Union zu unterstützen. Das Europäische Gremium für Künstliche Intelligenz „soll die Kommission dabei unterstützen, KI-Kompetenzinstrumente sowie die Sensibilisierung und Aufklärung der Öffentlichkeit in Bezug auf die Vorteile, Risiken, Schutzmaßnahmen, Rechte und Pflichten im Zusammenhang mit der Nutzung von KI-Systemen zu fördern. In Zusammenarbeit mit den einschlägigen Interessenträgern sollten die Kommission und die Mitgliedstaaten die Ausarbeitung freiwilliger Verhaltenskodizes erleichtern, um die KI-Kompetenz von Personen, die mit der Entwicklung, dem Betrieb und der Verwendung von KI befasst sind, zu fördern."

II. Der rechtswissenschaftliche Stand zur KI-Kompetenz

Es gibt zwar erste Kommentarliteratur zur KI-VO und einzelne Aufsätze zur KI-Kompetenz. Eine Reihe der angekündigten Kommentare zur KI-VO ist aber bisher noch nicht erschienen. Es ist daher derzeit schwer, von einer herrschenden Meinung zu sprechen.

Der Umfang der notwendigen KI-Kompetenz richtet sich nach derzeitigem Forschungsstand nach den drei Kriterien: Zweck, Risiko und Einsatzkontext.[6] KI-Kompetenz soll auch rechtliche Kenntnisse hinsichtlich der Anforderungen und Definitionen der KI-VO umfassen – wozu insbesondere der Begriff des KI-Systems und die verschiedenen Risikoklassen zählen.[7]

KI-Kompetenz innerhalb einer Organisation soll auch arbeitsteilig erfüllt werden können. Sind mehrere Personen etwa an der Entwicklung oder dem Einsatz eines KI-Systems beteiligt, so soll es möglich sein, dass die einzelnen Personen nur über die KI-Kompetenz verfügen, die für ihre einzelnen Aufgaben erforderlich sind, wenn in der Organisation insgesamt eine ganzheitliche KI-Kompetenz sichergestellt ist.[8] Daher soll es etwa möglich sein, dass die Kenntnis der rechtlichen Anforderungen durch eine Rechtsabteilung oder externe Berater erfüllt werden kann.[9]

III. FAQ der Kommission

Die Europäische Kommission[10] ist laut ihrer FAQ[11] der Auffassung, dass die KI-Kompetenz alle Personen in der Organisation betrifft, die direkt mit einem KI-System zu tun haben. Die Pflicht gilt nicht nur hinsichtlich eigener Mitarbeiter:innen, sondern auch bezüglich Personen, die im weiteren Sinne dem organisatorischen Zuständigkeitsbereich unterstehen. Dabei kann es sich beispielsweise um Auftragnehmer, Dienstleister oder auch Kunden handeln.

Laut Kommission besteht keine Verpflichtung, die konkreten KI-Kenntnisse der Mitarbeiter:innen zu messen. Unter Berücksichtigung der technischen Kenntnisse, Erfahrungen, Ausbildung und Schulung der Mitarbeiter soll aber ein ausreichendes Maß an KI-Kompetenz sichergestellt werden. Die KI-Kompetenz erstreckt sich auf Anwendungen wie ChatGPT – so sollte etwa über das Risiko von Halluzinationen aufgeklärt werden.

Die Kommission macht keine starren Vorgaben für die Umsetzung der KI-Kompetenz. Angesichts der Breite des Themas und der sich rasch entwickelnden Technologie hält sie ein gewisses Maß an Flexibilität für erforderlich. Um die gesetzlichen Anforderungen zu erfüllen, empfiehlt sie jedoch vier Handlungsschritte: KI-Verständnis entwickeln, die Rolle der Organisation definieren, konkrete KI-Risiken identifizieren und konkrete KI-Kompetenz-Maßnahmen entwickeln. Zum KI-Verständnis gehören Kenntnisse zur Funktion von KI, zu ihrem Einsatz innerhalb der Organisation, aber auch zu potenziellen Chancen und Risiken von KI. Bei der Rolle der Organisation geht es darum, dass ein Verständnis

6 Kaufmann in: BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Art. 4.

7 Unter Bezugnahme auf die FAQ der Kommission: Kaufmann in: BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Art. 4, Rn. 31.

8 Kaufmann in: BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Art. 4, Rn. 34.

9 Ebenda.

10 Der für die Umsetzung der KI-VO zuständige Teil der Kommission ist das KI-Büro.

11 Siehe fn. 2.

darüber entwickelt wird, ob eine Organisation selbst KI entwickelt, benutzt oder vertreibt. Bei der Identifizierung der konkreten KI-Risiken sollte klargestellt werden, welche Informationen Mitarbeiter:innen zu den konkret eingesetzten KI-Systemen haben sollten. Darüber hinaus sollte geklärt werden, welche Risiken die Mitarbeitenden kennen müssen und über welche Risikominderungsmaßnahmen sie informiert sein sollten. Der letzte Schritt sollte auf den vorangegangenen Schritten aufbauen – Unterschiede in Bezug auf technisches Wissen, Erfahrung, Ausbildung und Schulung sollten berücksichtigt werden. Was wissen die einzelnen Personen und was sollten sie darüber hinaus noch wissen? Dann sollte der konkrete Kontext des KI-Einsatzes definiert werden. Die Kommission empfiehlt bei all diesen Schritten ein Vorgehen, das nicht nur auf die Einhaltung des Rechtsrahmens – sondern auch auf allgemeine ethische Erwägungen abstellt.

Sollte es sich um ein KI-System handeln, das ein Hochrisiko-KI-System im Sinne der KI-VO ist, sollten weitergehende Überlegungen bezüglich der KI-Kompetenz angestellt werden. Das bloße Lesen und Einhalten der Gebrauchsanleitung eines KI-Systems kann unter Umständen nicht ausreichend sein, um die KI-Kompetenz zu gewährleisten. Empfohlen werden Schulungen und Leitlinien, die dem Kenntnisstand und der Art der Kenntnisse der jeweiligen Zielgruppe sowie dem Kontext und dem Zweck der in der Organisation verwendeten KI-Systeme am besten entsprechen. Die Anforderungen an KI-Schulungen sind abhängig vom Einsatzkontext und dem Wissensstand der Teilnehmer:innen.

Bisher schreibt die Kommission keine sektorspezifischen KI-Kompetenzmaßnahmen vor. Der Sektor als Kontext sollte zusammen mit dem jeweiligen Risiko bei der Entwicklung einer Initiative zur Förderung der KI-Kompetenz berücksichtigt werden. Personen, die für Dienstleister:innen oder Auftragnehmer:innen tätig sind, müssen über die gleichen KI-Kenntnisse verfügen wie die Mitarbeiter:innen.

Dass eine Person Vorkenntnisse im Bereich KI hat – etwa bei der Entwicklung eines KI-Systems oder -Modells involviert war – führt nicht automatisch dazu, dass sie KI-Kompetenz besitzt. KI-Kompetenz umfasst Wissen über Chancen und Risiken der spezifisch eingesetzten KI-Systeme. Es reicht daher nicht aus, dass Wissen über irgendeine Art von KI-System vorhanden ist. Zudem sollten bei Bedarf ethische und rechtliche Grundlagen vermittelt werden.

Die KI-VO schreibt im Rahmen der KI-Kompetenz nicht den Erwerb eines KI-Zertifikats (oder Ähnliches) vor. Die interne Dokumentation über KI-Schulungen ist demnach ausreichend. Zudem bedarf es keines „KI-Beauftragten". Eine Rolle, die der des Datenschutzbeauftragten aus der Datenschutz-Grundverordnung (DSGVO) entspricht, sieht die KI-VO nicht vor.

IV. Hochschul-Compliance und KI-Kompetenz

Hochschulen sollten sich mit den FAQ der Kommission auseinandersetzen und überlegen, ob sie die vorgeschlagenen Handlungsschritte auf ihre internen Prozesse übertragen können. Bei KI-Systemen, die Studierende betreffen, sollte das Recht auf Bildung stets mitgedacht werden. Aufgrund der möglicherweise langfristigen Folgen für Studierende und deren Berufsleben sollten Risiken von KI-Systemen im Bereich der Lehre und Hochschulverwaltung besonders genau betrachtet werden.
Noch weithin ungeklärt ist, wie mit sogenannter Schatten-KI im Rahmen der Verpflichtung zur KI-Kompetenz umgegangen werden muss. Schatten-KI bezeichnet in diesem Zusammenhang den Einsatz von KI-Systemen durch Mitarbeiter:innen, um Arbeitsaufgaben zu erledigen – ohne dass der Einsatz der KI offiziell angeordnet oder gestattet worden ist.

V. Durchsetzung der KI-Kompetenz

Die Durchsetzung der KI-Kompetenz liegt in der Zuständigkeit der Mitgliedstaaten. In Deutschland soll voraussichtlich die Bundesnetzagentur die zuständige Aufsichtsbehörde für die Einhaltung der KI-VO werden. Solange das entsprechende deutsche Durchführungsgesetz nicht vorliegt, können aber auch keine näheren Ausführungen zur deutschen Aufsichtsstruktur gemacht werden. Das Thema wird deshalb zu einem späteren Zeitpunkt in einem Infobrief behandelt.

Die Kommission stellt in ihren FAQ klar, dass im Schadensfall Anbieter oder Betreiber eines KI-Systems nach nationalem Recht haftbar gemacht werden können. Die KI-VO schaffe aber weder eigene Straftatbestände noch einen originären Anspruch auf Schadenersatz.

VI. Lebendes KI-Archiv

Die EU-Kommission hat ein sogenanntes „living repository“[12] zur KI-Kompetenz gegründet.[13] Dort werden Praxisbeispiele für laufende Praktiken zur Förderung der KI-Kompetenz veröffentlicht. Die Liste der dort aufgeführten Praktiken ist ausdrücklich nicht abschließend – es handelt sich lediglich um Beispiele, die laufend aktualisiert werden sollen. Dargestellt werden Praktiken mit unterschiedlichem Umsetzungsgrad: etwa vollständig umgesetzt, teilweise eingeführt, geplant.

Das lebende KI-Archiv ist zwar Teil der Bemühungen der Kommission, die Normadressat:innen bei der Einhaltung der KI-VO zu unterstützen, aber es handelt sich nicht um offizielle rechtsverbindliche Hinweise. Die Kommission weist ausdrücklich darauf hin, dass das Übernehmen der in dem Archiv dokumentierten Praktiken nicht automatisch eine Compliance mit den Anforderungen an die KI-Kompetenz garantiert. Die Veröffentlichung der Praktiken durch die Kommission stellt weder eine Empfehlung noch eine Bewertung dar. Das Instrument ist als öffentliches Lern- und Austauschforum gedacht.

Als weitere Maßnahme zur Förderung der KI-Kompetenz ist eine eigene Webseite zum Thema KI-Kompetenzen und -Fähigkeiten derzeit in Vorbereitung. Die Kommission hat Anfang des Jahres ein Webinar zum Thema KI-Kompetenz durchgeführt, das aufgezeichnet wurde und noch weiterhin abrufbar ist.[14]

12 Der Begriff kann mit „lebendes Archiv“ übersetzt werden – zum Teil wird auch der Begriff „lebendes Repository“ verwendet..

13 EU-Kommission, Living repository to foster learning and exchange on AI literacy, 04.02.2025, abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy.

14 EU-Kommission, Third AI Pact webinar on AI literacy, 20.02.2025, https://digital-strategy.ec.europa.eu/de/events/third-ai-pact-webinar-ai-literacy.

Urteile für alle

Zur Haftung der freien Rechtsprechungsdatenbank openJur für einen Datenschutzverstoß

Von Nikolaus von Bernuth, Berlin

Das gemeinnützige Projekt openJur veröffentlicht Gerichtsentscheidungen, um sie der Allgemeinheit zugänglich zu machen. Dafür fragt die Plattform Urteile bei Gerichten direkt an. Regelmäßig liest sie jedoch auch aus amtlichen Datenbanken aus und veröffentlicht automatisiert. In einem auf diese Weise publizierten Urteil waren persönliche Daten nicht ausreichend anonymisiert – die betroffene Person verklagte openJur daraufhin. Die existenzbedrohende Klage wurde nun durch das Landgericht (LG) Hamburg abgewiesen. Die Entscheidung hat übergeordnete Bedeutung für Projekte, die sich für freies und offenes Wissen einsetzen.

I. Zugänglichkeit von Gerichtsentscheidungen

Gerichtsverfahren sowie Urteilsverkündungen deutscher Gerichte sind grundsätzlich öffentlich, dies ergibt sich aus §§ 169, 173 Gerichtsverfassungsgesetz (GVG). Auch Art. 6 der Europäischen Menschenrechtskonvention (EMRK) gewährleistet den Grundsatz der Öffentlichkeit. Dementsprechend stellte der Bundesgerichtshof (BGH) im Jahr 2017 ausdrücklich klar, dass auch der Inhalt dieser Urteile öffentlich ist: „Gerichtsentscheidungen unterliegen nicht der Geheimhaltung". Vielmehr gilt nach Ansicht des BGH: „Die Weitergabe anonymisierter Entscheidungsabschriften an Dritte ist […] Teil der öffentlichen Aufgabe der Gerichte, Entscheidungen zu veröffentlichen."[1] In gleichem Sinne urteilten auch das Bundesverwaltungsgericht und das Bundesverfassungsgericht.[2]

In der Praxis ist bisher aber nur ein kleiner Teil der tagtäglich ergehenden Gerichtsentscheidungen öffentlich zugänglich. Nach einer Studie des Rechtswissenschaftlers Prof. Dr. Hanjo Hamann aus dem Jahr 2021 wird pro Jahr weniger als 1 % aller Gerichtsentscheidungen, die eine Begründung enthalten, veröffentlicht.[3] Gerade Urteile der Gerichte unterer Instanzen (Amtsgericht, Landgericht, Verwaltungsgericht, Arbeitsgericht, Sozialgericht, Finanzgericht) finden sich meist nicht in Datenbanken wieder. Oft fehlt es in diesen „einfachen" Verfahren auch an einem öffentlichen Interesse an der Entscheidung. Doch auch Urteile unterer Instanzen, etwa von Verwaltungsgerichten, die über Auflagen und Verbote von Versammlungen entscheiden, können Auswirkungen auf eine Vielzahl von Personen haben und ein öffentliches Interesse begründen. Das gilt ebenso in Fallkonstellationen, die noch nicht durch die höchsten Gerichte entschieden wurden. Große Aufmerksamkeit erregte etwa die LAION-Entscheidung des LG Hamburg zur Zulässigkeit des Trainings von KI-Modellen mit urheberrechtlich geschützten Werken.'[4]

---

1 BGH, Beschluss vom 05.04.2017 - IV AR(VZ) 2/16, Rn. 16.

2 BVerfG, Beschluss vom. 14.09.2015 - 1 BvR 857/15; BVerwG, Urteil vom 26.02.1997 - 6 C 3.96. Aus der Literatur insbesondere: Hamann, JZ 2021, 656.

3 Die Studie untersuchte die ordentliche Gerichtsbarkeit und ist publiziert in Hamann, JZ 2021, 656; vgl. hierzu auch Hamann, LTO, https://www.lto.de/recht/justiz/j/studie-veroeffentlichung-gerichtsentscheidungen-deutschland-transparenz-justiz (alle Links dieses Beitrags zuletzt abgerufen am 10.06.2025).

4 LG Hamburg, Urteil vom 27.9.2024 – 310 O 227/23. Dazu Müller, Die Menge macht's, DFN-Infobrief Recht 11/2024. Vertiefend Radeisen/Suilmann, ZUM 2025, 74.

So ist es erneut eine Entscheidung des LG Hamburg[5], die hier näher vorgestellt werden soll. Es handelt sich um einen Fall mit grundsätzlicher Bedeutung für die Zugänglichkeit von Gerichtsentscheidungen. Im Kern drehte sich das Verfahren um die Frage der Haftung für Datenschutzverstöße bei der Verbreitung von Gerichtsentscheidungen. Zugleich beschäftigte sich das Gericht in diesem Zuge mit der Reichweite des sogenannten Medienprivilegs in Art. 85 Abs. 2 Datenschutz-Grundverordnung (DSGVO).

II. Die Sachlage

Die Klage richtete sich gegen openJur. Unter diesem Namen betreibt ein gemeinnütziges Projekt[6] eine Online-Datenbank, in der Gerichtsentscheidungen veröffentlicht werden. Dafür greift openJur zum einen auf öffentliche Entscheidungsdatenbanken zu, verbreitet also gesammelt bereits veröffentlichte Entscheidungen. Zum anderen fragt das Projekt auch einzelfallbezogen Kopien relevanter Entscheidungen bei Gerichten an, die auf der Plattform dann erstveröffentlicht werden.

Gegenstand des Streits vor dem LG Hamburg war die Veröffentlichung einer verwaltungsgerichtlichen Entscheidung. OpenJur hatte die Entscheidung automatisiert aus einer amtlichen Datenbank des Landes Berlin übernommen und auf der eigenen Plattform zur Verfügung gestellt.

Die Entscheidung war jedoch nicht anonymisiert. Entgegen dem üblichen Verfahren hatte die Justiz die Entscheidung vor Veröffentlichung in der amtlichen Datenbank nicht anonymisiert. Daher waren der Klarname und weitere Details zu den persönlichen Verhältnissen des Verfahrensbeteiligten offen einsehbar. Im Zuge der automatisierten Veröffentlichung übernahm dann auch openJur das Urteil in nicht anonymisierter Form in die eigene Datenbank.

Es gibt keine pauschalen, einheitlichen Vorgaben, wie Gerichtsentscheidungen veröffentlicht werden sollen. Es entspricht jedoch der Regel, dass zumindest Informationen zu natürlichen Personen, die sie identifizierbar machen, weitestmöglich entfernt werden.[7] Rechtlich bestehen zwar Zweifel daran, ob Gerichtsentscheidungen stets anonymisiert werden müssen oder sollten – schon, weil diese Abwägungsentscheidung kapazitätsmäßig nicht in jedem Fall getroffen werden kann, veröffentlichen die öffentlichen Stellen in aller Regel anonymisiert.

Nachdem die betroffene Person von dem abrufbaren Urteil Kenntnis erlangt hatte, mahnte sie openJur wegen der Preisgabe ihrer personenbezogenen Daten ab. Wie auch das LG Hamburg anmerkte, handelte es sich um potenziell geschäftsschädigende personenbezogene Informationen. OpenJur anonymisierte auf den Hinweis hin noch am selben Tag das betreffende Urteil in der eigenen Datenbank. Dennoch erhob der Betroffene Klage vor dem LG Hamburg. Er begehrte von der Plattform Ersatz der Abmahnkosten, Unterlassung der Veröffentlichung seiner Daten sowie Schmerzensgeld wegen des eingetretenen immateriellen Schadens.[8]

III. Die grundsätzliche Bedeutung des Falls

Der Fall dreht sich im Kern um zivilrechtliche Haftungsfragen. Ist die Datenbank dafür verantwortlich, eine nicht anonymisierte Gerichtsentscheidung aus einer öffentlichen Datenbank übernommen und ungeprüft veröffentlicht zu haben?

Die Entscheidung ist bedeutsam, da openJur als gemeinnütziges, nicht gewinnorientiertes Projekt einen wichtigen Beitrag zur Zugänglichkeit von Wissen leistet. Gerichtsentscheidungen, die sonst entweder überhaupt nicht veröffentlicht werden oder in schwer auffindbaren öffentlichen Datenbanken unentdeckt bleiben, kommen so an die Öffentlichkeit. Wäre openJur jedoch nach den Maßstäben dieses Falls haftbar, so könnte das

5 LG Hamburg, Urteil vom 09.05.2025 - 324 O 278/23, abrufbar unter: https://openjur.de/u/2517464.html.

6 Der zunächst als eingetragener Verein organisierte Träger hat inzwischen, in Reaktion auf die Haftungsrisiken, eine gemeinnützige GmbH gegründet.

7 Dazu Hoeren/Rombach/John, Auch beim Schwärzen gibt es Graustufen, DFN-Infobrief Recht 05/2023;Kaufmann/Uharek, LTO, https://www.lto.de/recht/justiz/j/anonymisierung-gerichtsentscheidungen-urteile-namen-schwaerzen-persoenlichkeitsrecht-informationsfreiheit und Hamann, LTO, https://www.lto.de/recht/justiz/j/studie-veroeffentlichung-gerichtsentscheidungen-deutschland-transparenz-justiz.

8 Der Sachverhalt aus Perspektive beider Parteien ist im veröffentlichten Urteil ausführlich dargestellt, LG Hamburg, Urteil vom 09.05.2025 - 324 O 278/23, Rn. 6-32.

gemeinnützige, spendenbasierte Projekt nach eigener Darstellung nicht weiterbetrieben werden.[9] Ähnliche Projekte der offenen Zurverfügungstellung von Wissen könnten ebenso bedroht sein. OpenJur hat nach eigenen Angaben bereits mehr als 625.000 Entscheidungen im Volltext veröffentlicht, die über 400 Millionen Mal abgerufen wurden. Damit leistet die Datenbank einen erheblichen Beitrag zur Verwaltung, Konservierung und Zugänglichkeit von Wissen – und ist ein wichtiges Informationsportal für die Rechtswissenschaft. Die individuell angefragten und erstveröffentlichten Entscheidungen prüft und anonymisiert sie einzeln. Im Falle der automatisiert veröffentlichten Entscheidungen, die in großer Menge aus amtlichen Datenbanken übernommen werden, kann openJur dies nicht gewährleisten.

IV. Die Entscheidungsgründe

Im Ergebnis hat das LG Hamburg die Klage gegen openJur vollumfänglich abgewiesen – die Plattform muss in dieser Konstellation nicht haften. In den Urteilsgründen hat es sich intensiv mit der datenschutzrechtlichen Haftung in Bezug auf die verschiedenen geltend gemachten Ansprüche (Unterlassung, Schmerzensgeld, Abmahnkosten) auseinandergesetzt.

1. Unterlassungsanspruch nach der DSGVO

Zum einen hat der Betroffene von der Plattform verlangt, es zu unterlassen, seine personenbezogenen Daten wie in der oben beschriebenen Weise geschehen im Internet zu verbreiten. Ein solcher Unterlassungsanspruch kann sich aus Art. 17 DSGVO ergeben. Das Gericht prüfte allerdings vorab, ob die DSGVO in der konkreten Konstellation überhaupt anwendbar ist. Die DSGVO sieht verschiedene Bereichsausnahmen vor, in denen die DSGVO nicht oder nur eingeschränkt gilt. Stattdessen greift dann möglicherweise nationales Recht.

Das Gericht prüfte im vorliegenden Verfahren die Bereichsausnahme in Art. 85 Abs. 2 DSGVO. Demnach sehen die Mitgliedstaaten für die Verarbeitung von Daten zu journalistischen Zwecken abweichende Regelungen vor. Im Umkehrschluss soll die DSGVO in diesen Fällen keine Anwendung finden, sondern die abweichenden nationalen Regelungen, die einen Ausgleich zwischen Pressefreiheit und Datenschutz herstellen sollen.

Damit diese Ausnahme von der DSGVO greift, muss es sich also bei der Tätigkeit von openJur um eine journalistische Tätigkeit im Sinne des Art. 85 Abs. 2 DSGVO handeln. Dies prüfte das LG Hamburg eingehend.[10] Der Begriff ist nach europarechtlichem Begriffsverständnis auszulegen und demnach weit zu verstehen, wie sich aus Erwägungsgrund 153 zur DSGVO ergibt.

Nach dem Europäischen Gerichtshof (EuGH) ist insbesondere das Ziel der Veröffentlichung maßgeblich: Die Veröffentlichung muss zum Ziel haben, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten. Zugleich stellt der EuGH einerseits fest, dass nicht jede Veröffentlichung im Internet eine journalistische Tätigkeit darstellt. Andererseits ist weder eine berufliche Tätigkeit noch die Anbindung an eine Redaktion erforderlich.[11]

OpenJur betreibt nach Ansicht des LG Hamburg einen Intermediärsdienst, verbreitet also fremde Inhalte an die Allgemeinheit. Im Unterschied etwa zu Online-Plattformen werden jedoch nicht nutzergenerierte Inhalte verbreitet, sondern spezifisch nur Gerichtsentscheidungen. Dies kann als journalistische Tätigkeit eingeordnet werden, wenn ein Mindestmaß an Bearbeitung geleistet wird, so das LG Hamburg mit Verweis auf rechtswissenschaftliche Literatur.[12] Es weist aber auch auf zwei Entscheidungen des BGH hin, die einem Ärztebewertungsportal das Medienprivileg versagten.[13]

Anhand dieser Maßstäbe kam das LG Hamburg zu dem Ergebnis, dass die Bereichsausnahme greife, openJur also journalistische

9 Zur Einschätzung von openJur: https://openjur.de/i/openjur_wird_verklagt.html.

10 LG Hamburg, Urteil vom 09.05.2025 - 324 O 278/23, Rn. 38ff.

11 EuGH, Urt. v. 14.02.2019 - C-345/17, Rn. 59 – Buivids; BeckOK InfoMedienR/Cornils, 47. Ed. 1.2.2021, Art. 85 DSGVO, Rn. 70.

12 LG Hamburg, Urteil vom 09.05.2025 - 324 O 278/23, Rn. 40.

13 BGH, Urteil vom 23.09.2014 - VI ZR 358/13 – Ärztebewertungsportal II; BGH, Urteil vom 20.02.2018 - VI ZR 30/17 – Ärztebewertungsportal III.

Zwecke verfolge.[14] Dabei knüpft das Gericht maßgeblich daran an, dass openJur auch nach Relevanz individuell ausgewählte Entscheidungen anfragt, gegebenenfalls sogar gerichtlich erstreitet und veröffentlicht. Zudem verfasse die Plattform eigene Orientierungssätze und Schlagworte. In der Rubrik „Aktuell" würden besonders relevante Entscheidungen kuratiert. Damit gehe die Tätigkeit über das bloße Datensammeln und Verbreiten von Drittinhalten hinaus.

Gerade im vorliegenden Fall handelte es sich hingegen nicht um eine individuell ausgewählte, sondern um eine automatisiert veröffentlichte Entscheidung. Dies sieht auch das LG Hamburg, bleibt aber bei seiner Einschätzung. Die unterschiedlich gesammelten Entscheidungen seien in der Darbietung nicht voneinander getrennt und ergäben so ein Angebot, das im Gesamteindruck den nötigen redaktionell geprägten Charakter aufweise.

Das Gericht weist zudem darauf hin, dass neben dem journalistischen Zweck wohl auch die Bereichsausnahme für wissenschaftliche Zwecke gegriffen hätte (Art. 85 Abs. 2 DSGVO). Dies begründe sich mit der bereits erwähnten Bedeutung der openJur-Datenbank für die Rechtswissenschaft, die sich auch im Selbstverständnis der Plattform widerspiegelt.[15]

Im Ergebnis wird der Unterlassungsanspruch aus Art. 17 DSGVO daher schon mangels Anwendbarkeit der DSGVO von vornherein abgelehnt.

2. Unterlassungsanspruch nach nationalem Recht

Das LG Hamburg prüft anschließend auch einen Unterlassungsanspruch jenseits der DSGVO aus nationalem Recht. Ein solcher Anspruch könnte sich aus §§ 823 Abs. 1, 1004 Abs. 1 S. 2 Bürgerliches Gesetzbuch (BGB) analog, Art. 2 Abs. 1, Art. 1 Abs. 1 Grundgesetz (GG) ergeben.
Das Gericht macht zunächst deutlich, dass die Veröffentlichung der personenbezogenen Daten in der Tat eine Verletzung des Allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1, Art. 1 Abs. 1 GG darstellte. Doch diese Verletzung führt nur zu weiteren Ansprüchen, wenn sie auch rechtswidrig war.

Das LG Hamburg befand, dass openJur nicht rechtswidrig handelte. Die Plattform nutzte eine sogenannte „privilegierte Quelle" und handelte damit gerechtfertigt. Das Institut der „privilegierten Quelle" ist im Presserecht anerkannt und entbindet für bestimmte Berichterstattung und Äußerungen von journalistischen Sorgfaltspflichten. Hier übernahm openJur die Entscheidung aus einer amtlichen Datenbank. Mitteilungen staatlicher Institutionen stellen einen klassischen Fall privilegierter Quellen dar. Medien sollen sich darauf verlassen dürfen, dass die dort enthaltenen Informationen rechtmäßig sind und bereits vor der Veröffentlichung eine Grundrechtsabwägung stattgefunden hat. Im konkreten Fall hatte openJur keine Anhaltspunkte, dass die amtliche Datenbank nicht anonymisierte Entscheidungen veröffentlichte. Daher konnte die Plattform die Entscheidung im Vertrauen auf die privilegierte Quelle rechtmäßig veröffentlichen. Ein Unterlassungsanspruch wurde insgesamt abgelehnt.

3. Schadensersatzanspruch (Schmerzensgeld)

Der Kläger wollte von openJur zudem Schadensersatz in Form von Schmerzensgeld erlangen. Das Gericht stellt hier klar, dass die Veröffentlichung aus den bereits ausgeführten Gründen nicht rechtswidrig war und daher auch kein Anspruch auf Schadensersatz besteht.

Doch der Kläger prangerte nicht nur die Veröffentlichung an, sondern argumentierte zudem, dass openJur seinem Auskunftsanspruch nach Art. 15 DSGVO zu spät nachgekommen sei. Danach kann jede betroffene Person von der datenverarbeitenden Stelle Auskunft über diverse Umstände der Datenverarbeitung verlangen. Diese Auskunft hat unverzüglich, regelmäßig innerhalb eines Monats, zu erfolgen. OpenJur hatte das Auskunftsgesuch kurz nach der Mitteilung bereits teilweise beantwortet und die personenbezogenen Daten entfernt, allerdings erst rund fünf Monate im Rahmen des gerichtlichen Verfahrens vollständig Auskunft erteilt.

Der Kläger versuchte glaubhaft zu machen, hierdurch sei ein Gefühl des Kontrollverlusts an seinen Daten und damit ein immaterieller Schaden entstanden.[16] Die Voraussetzungen für einen immateriellen Schaden nach Datenschutzverstoß wurden zuletzt

14 LG Hamburg, Urteil vom 09.05.2025 - 324 O 278/23, Rn. 41ff.

15 LG Hamburg, Urteil vom 09.05.2025 - 324 O 278/23, Rn. 47.

16 Siehe dazu EuGH, Urt. v. 04.10.2024 – C-200/23, Rn. 145, 156 i.V.m. 137.

durch höhere Rechtsprechung in mehreren Entscheidungen konkretisiert.[17] Demnach reicht ein einfacher Verstoß gegen die DSGVO nicht, andererseits ist kein bestimmter Grad an Schwere oder Erheblichkeit erforderlich - der bloße Datenverlust kann bereits einen Schaden begründen.[18]

Nach diesen Maßstäben stellte das LG Hamburg hier keinen immateriellen Schaden fest. OpenJur hatte bereits wenige Minuten nach Eingang der Beschwerde das Auskunftsbegehren in den relevanten Teilen beantwortet, sodass es nicht glaubhaft erschien, dass die fehlenden Auskunftsangaben alleine einen relevanten Schaden bei dem Betroffenen ausgelöst haben.

4. Abmahnkosten

Zuletzt lehnt das LG Hamburg auch einen Anspruch auf Ersatz der Abmahnkosten, also der vorgerichtlichen Rechtsverfolgungskosten, ab. Diese wären nur ersatzfähig, wenn die geltend gemachten Unterlassungs- oder Schadensersatzansprüche begründet gewesen wären.

V. Fazit

OpenJur konnte sich gegen eine Haftung erfolgreich zur Wehr setzen. Interessant an dem Verfahren ist, dass das Gericht ein sehr weites Verständnis des datenschutzrechtlichen Medienprivilegs zugrunde legt. Zu beachten ist, dass openJur davon profitierte, weil die Plattform in gewissem Maße auch redaktionelle Gestaltungsentscheidungen trifft. Zudem lässt das Gericht aber auch anklingen, dass das Privileg zugunsten wissenschaftlicher Verarbeitungszwecke ebenfalls hätte greifen können.

Die Entscheidung gibt zum einen openJur Rechtssicherheit beim Betrieb der freien Datenbank. Auch für andere Datenbanken, die Daten aus amtlichen Quellen beziehen, dürfte sie ein positives Signal sein. Damit wurde insgesamt das freie Wissen im Internet gestärkt.

Hierin liegt auch die wesentliche Bedeutung des Falls für die Wissenschaft. Gerade die Rechtswissenschaft profitiert von freien Datenbanken wie openJur, um an Forschungsmaterial zu gelangen. Doch auch in anderen Disziplinen ist die Verfügbarkeit von Daten und Wissen elementar für die wissenschaftliche Arbeit.

---

17 Dazu ausführlich: Müller, Kurzbeitrag: Keine Geschenke vom Bundesarbeitsgericht, DFN-Infobrief Recht 12/2024; Tech, Wer den Schaden hat, braucht für den Ärger nicht zu sorgen, DFN-Infobrief Recht 08/2024; Müller, Ist das denn meine Schuld?, DFN-Infobrief Recht 06/2024; Müller, Ich glaub, es hackt, DFN-Infobrief Recht 04/2024; Voget, Kurzbeitrag: Nicht (un)erheblich?!, DFN-Infobrief Recht 07/2023.

18 LG Hamburg, Urteil vom 09.05.2025 - 324 O 278/23, Rn. 64.

DFN Infobrief-Recht-Aktuell

- ## KI-Recht: Verhaltenskodex für KI mit allgemeinem Verwendungszweck seit 10. Juli 2025 verfügbar

  Am 2. August 2025 treten die Regelungen des KI-Gesetzes in Kraft. Der von unabhängigen Sachverständigen erstellte KI-Verhaltenskodex ist als Hilfe für die Industrie gedacht, um die Regelungen des KI-Gesetzes einzuhalten. Er besteht aus drei Kapiteln: Transparenz, Urheberrecht sowie Sicherheit und Schutz. Anbieter von KI-Modellen mit allgemeinem Verwendungszweck können den Kodex freiwillig unterzeichnen und die Einhaltung der einschlägigen Verpflichtungen aus dem KI-Gesetz durch Einhaltung des Kodex nachweisen.

  Hier erhalten Sie den Link zur Pressemitteilung: https://ec.europa.eu/commission/presscorner/detail/de/ip_25_1787

- ## Mietrecht/Strafrecht: Nicht jede heimliche Aufnahme einer Person in ihrer Wohnung führt zu einer Strafbarkeit nach § 201a Abs. 1 S. 1 Strafgesetzbuch (StGB)

  Das Oberlandesgericht Hamm schloss sich mit Urteil vom 18. März 2025 der Rechtsprechung des Bundesgerichtshofs an. Nach dieser Rechtsprechung bedarf es zusätzlich zur Herstellung von Bildaufnahmen eines (Verletzungs-)Erfolgs in Form einer dadurch bewirkten Verletzung des höchstpersönlichen Lebensbereichs der abgebildeten Person. Denn es handele sich bei § 201a StGB um ein Erfolgsdelikt. Situationen, die zwar der Privatsphäre zuzuordnen sind, aber ein neutrales Verhalten zeigen, benötigen danach keinen strafrechtlichen Schutz.

  Hier erhalten Sie den Link zur Entscheidung:
  https://nrwe.justiz.nrw.de/pdfdownload/downloadEntscheidung.php?entscheidung=/nrwe/olgs/hamm/j2025/4_ORs_24_25_Beschluss_20250318.html

- ## Datenschutzrecht/Arbeitsrecht: Verzicht auf Auskunftsverlangen nach Art. 15 Datenschutz-Grundverordnung durch Abgeltungsklausel aus arbeitsvertraglichem Vergleich

  Das Oberverwaltungsgericht Saarlouis entschied mit Urteil vom 13. Mai 2025, dass kein Anspruch auf Auskunft gegen die ehemalige Arbeitgeberin mehr bestünde, soweit der Arbeitnehmer in einem arbeitsgerichtlichen Vergleich eine Abgeltungsklausel unterzeichnet hat, die sämtliche Ansprüche aus dem Arbeitsverhältnis umfasst.

  Hier erhalten Sie den Link zur Entscheidung:
  https://recht.saarland.de/bssl/document/NJRE001609667/format/xsl/part/L/anchor/resultlistentry0?oi=eheb2WGsbG&sourceP=%7B%22position%22%3A0%2C%22sort%22%3A%22juris%22%2C%22source%22%3A%22TL%22%7D

Kurzbeitrag: Rote Karte für den Betriebsratsvorsitzenden

Weiterleitung sensibler Personaldaten an private E-Mail-Adresse als grobe Pflichtverletzung

von Marc-Philipp Geiselmann, Münster

Das Hessische Landesarbeitsgericht bestätigte in seinem Beschluss vom 10. März 2025 (Aktenzeichen: 16 TaBV 109/24), dass die Weiterleitung sensibler Personaldaten an einen privaten E-Mail-Account durch ein Betriebsratsmitglied einen groben Pflichtverstoß darstellt, der zum Ausschluss aus dem Betriebsrat führen kann. Der Fall verdeutlicht die hohen datenschutzrechtlichen Anforderungen an Betriebsratsmitglieder und die Konsequenzen von Verstößen.[1]

I. Sachverhalt: Systematische Datenschutzverstöße trotz Abmahnung

Der Betriebsratsvorsitzende einer Klinik mit rund 390 Mitarbeitern richtete eine automatische Weiterleitung aller dienstlichen E-Mails an seinen privaten GMX-Account ein. Nach einer Abmahnung im September 2023 wegen dieses Verhaltens leitete er im November 2023 erneut eine Excel-Liste mit hochsensiblen Personaldaten (Namen sämtlicher Mitarbeiter, Stellung im Betrieb, Zeitansatz, Tarifgruppe, Stufe, Grundentgelt, zeitlicher Stufenverlauf, Tarifeintritt, Eingruppierung, Vergleichsdaten zur Eingruppierung im Konzern, zum Grundgehalt im Konzern) von seinem dienstlichen an seinen privaten E-Mail-Account weiter, bearbeitete die Daten zu Hause und übersandte sie anschließend an den Betriebsrat. Der Arbeitgeber beantragte daraufhin seinen Ausschluss aus dem Betriebsrat gemäß § 23 Abs. 1 Betriebsverfassungsgesetz (BetrVG).

Der Betriebsratsvorsitzende rechtfertigte sein Vorgehen mit der Notwendigkeit, die Daten auf einem größeren privaten Bildschirm bearbeiten zu können und verwies auf technische Einschränkungen des dienstlichen Laptops. Zudem betonte er, die Daten seien auf seinem häuslichen Computer durch Passwörter und Sicherheitssoftware geschützt gewesen.

II. Rechtliche Beurteilung: Verstoß gegen § 79a BetrVG und die DSGVO

Das Gericht wies diese Argumentation zurück und stellte klar, dass Betriebsräte gemäß § 79a BetrVG und der Datenschutz-Grundverordnung (DSGVO) verpflichtet sind, personenbezogene Daten ausschließlich auf gesicherten dienstlichen Systemen zu verarbeiten. Die Weiterleitung der Tabelle erfolgte weder mit Einwilligung der Mitarbeiter (§ 26 Abs. 2 Bundesdatenschutzgesetz (BDSG)) noch war sie zur Aufgabenerfüllung erforderlich. Weiterhin verletzte die Weiterleitung an private Accounts ohne Einwilligung der Betroffenen oder anderweitige rechtliche Grundlage nach Art. 6 DSGVO nicht nur die Prinzipien der Rechtmäßigkeit und Transparenz nach Art. 5 DSGVO, sondern stelle auch einen Verstoß gegen die Datenminimierung dar. Zudem erhöhe die unkontrollierte Speicherung sensibler Informationen auf privaten Geräten das Risiko unbefugter Zugriffe erheblich, selbst wenn Sicherheitsvorkehrungen getroffen worden seien.

Entscheidend für die Qualifizierung als grobe Pflichtverletzung war die besondere Sensibilität der Gehaltsdaten, die Vorgeschichte mit der bereits erteilten Abmahnung sowie das systematische Umgehen von Sicherheitsvorkehrungen. Das Gericht betonte, dass selbst altruistische Motive wie eine effizientere

1 Zur fristlosen Kündigung eines Vorstandsmitglieds einer Aktiengesellschaft siehe Müller, Mehr Trennung zwischen Beruf und Privatem, DFN-Infobrief Recht 5/2025 abrufbar unter https://recht.dfn.de/wp-content/uploads/2025/05/Infobrief_Recht_5-2025.pdf (alle Links dieses Beitrags wurden zuletzt am 25.07.2025 abgerufen).

Bearbeitung keinen Datenschutzverstoß rechtfertigen. Der Betriebsratsvorsitzende hätte stattdessen den Arbeitgeber um technische Unterstützung – etwa einen Adapter für den Anschluss eines größeren Bildschirms – bitten müssen. Die Verfügbarkeit dienstlicher Ressourcen mache die private Datenverarbeitung entbehrlich.

III. Bedeutung des Beschluss

Mit der Bestätigung des Ausschlusses unterstrich das Gericht, dass das Vertrauen in die ordnungsgemäße Amtsführung nachhaltig gestört war. Datenschutzverstöße in Mitbestimmungsgremien seien kein Kavaliersdelikt, sondern könnten – unabhängig von einem konkreten Schadenseintritt – zum Verlust des Amtes führen.

Die Entscheidung sendet ein klares Signal an Betriebsräte, personenbezogene Daten ausschließlich auf dienstlichen, geschützten Systemen zu verarbeiten, und mahnt Arbeitgeber zugleich, die technische Ausstattung der Gremien bedarfsgerecht sicherzustellen. Regelmäßige Datenschutzschulungen und klare Compliance-Richtlinien bleiben unverzichtbar, um Rechtsverstöße zu vermeiden und das notwendige Vertrauen in die Betriebsratsarbeit zu wahren.

IV. Fazit

Der Beschluss stärkt den Schutz personenbezogener Daten im Betrieb und mahnt Betriebsratsmitglieder[2] zu besonderer Sorgfalt. Zugleich zeigt er auf, dass technische oder zeitliche Herausforderungen keine Rechtfertigung für rechtswidrige Datenverarbeitung bieten.

2 Zur Frage, ob Betriebsratsmitglieder auch Datenschutzbeauftragte sein dürfen siehe Tech, Betriebsratsmitglied als Datenschutzbeauftragter? „Nein!? Doch? Ohh!“, DFN-Infobrief Recht 9/2023 abrufbar unter:
https://recht.dfn.de/wp-content/uploads/2023/11/Infobrief_Recht_09-2023.pdf

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