„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

8 / 2026
August 2026

KI-Agenten im Recht

Agentische KI verspricht Automatisierung und Effizienz. Aber reichen unsere Gesetze, um ihren Gefahren Einhalt zu gebieten?

Elektronische Beweismittel ohne Grenzen

Die E-Evidence-Verordnung verschiebt im wahrsten Sinne des Wortes Grenzen bei der Erhebung elektronischer Beweismittel; betrifft sie auch Hochschulen?

Cyberresilienz auch für Hochschulen?

Die EU legt mit dem Cyber Resilience Act (CRA) einheitliche Cybersicherheitsanforderungen für Hard- und Software fest

Kurzbeitrag: Googeln verboten?

Die EU legt mit dem Cyber Resilience Act (CRA) einheitliche Cybersicherheitsanforderungen für Hard- und Software fest

KI-Agenten im Recht

Agentische KI verspricht Automatisierung und Effizienz. Aber reichen unsere Gesetze, um ihren Gefahren Einhalt zu gebieten?

Von Dr. Paul Friedl

KI-Agenten können heute Autos kaufen, Versicherungsfälle bearbeiten und Vermögen verwalten - und das weitgehend selbstständig. Diese Handlungsfähigkeit schafft neue Risiken. Ist das Recht gewappnet, um Programmfehlern, Datenverlust und Cyberangriffen vorzubeugen?

I. Was sind KI-Agenten?

Wer in den USA ein Auto kaufen will, sieht sich besonderen Schwierigkeiten ausgesetzt.[1] Komplizierte und intransparente Preisgestaltungen, die von Händler zu Händler variieren, führen zwar zu erheblichen Verhandlungsspielräumen. Wer nicht zu viel zahlen will, muss diese aber auch nutzen und durch cleveres Feilschen den oftmals massiv überhöhten ausgeschriebenen Preis nach unten drücken. Viel Arbeit also und unschön noch dazu. Das dachte sich auch der amerikanische Software-Engineer AJ Stuyvenberg, der deshalb das KI-System Clawdbot (heute OpenClaw) damit beauftragte, ihm beim Kauf des begehrten Hyundai Palisade unter die Arme zu greifen. Dazu ließ er das Programm zunächst Online-Foren für gute Preise durchstöbern, beauftragte es dann, Händler zu identifizieren, die das gewünschte Modell vorrätig hielten, und ließ es schließlich per E-Mail Angebote einholen, die es in einem letzten Schritt an die anderen Händler weiterleitete, um ein Bietergefecht auszulösen.[2] Am Ende konnte Stuyvenberg seinen erwünschten Zielpreis sogar noch unterbieten und den Wagen am nächsten Tag beim Händler abholen.

Agentic AI, zu Deutsch: Agentische KI oder KI-Agenten, werden Systeme wie das von Stuyvenberg genutzte OpenClaw[3] genannt. Gemeint ist damit Software, die auf KI-Modellen – regelmäßig sogenannten großen Sprachmodellen – aufbaut und großteils autonom Handlungen ausführen kann, um von Nutzer:innen vorgegebene Aufgaben zu erfüllen.[4]

Zentral für agentische KI sind dabei zwei Aspekte: zum einen die bereits angesprochene Selbstständigkeit. Diese drückt sich regelmäßig darin aus, dass das System zur Bewältigung von in menschlicher Sprache ausgedrückten Aufgabenstellungen[5] geeignete Softwarekapazitäten besitzt, beispielsweise die Fähigkeit, logisch zu denken, Computercode auszuführen oder mit Menschen zu kommunizieren. Zum anderen bedarf es für die Handlungsfähigkeit des Zugriffs auf oder der Einbindung in interne und externe Datensysteme, Software oder Schnittstellen: Im eingangs genannten Fall musste dem KI-System etwa erlaubt werden, frei im Internet zu surfen und E-Mails vom Account des Nutzers zu lesen und zu schreiben.

Derartige Kapazitäten werden auch als Tools bezeichnet, die einem KI-Agenten zur selbstständigen Benutzung zugänglich

---

1 Für eine mitreißende Darstellung der ortsüblichen Handelsbräuche aus Händlerperspektive, siehe This American Life, „129 Cars“, abrufbar unter https://www.thisamericanlife.org/513/129-cars (alle hier angegebenen Webseiten wurden zuletzt am 30. Juni 2026 abgerufen).

2 AJ Stuyvenberg, „Clawdbot bought me a car“, abrufbar unter <https://aaronstuyvenberg.com/posts/clawd-bought-a-car>.

3 „OpenClaw – Personal AI Assistant“, abrufbar unter <https://openclaw.ai/>.

4 Für einen guten Überblick über die verschiedenen Architekturen von KI-Agenten siehe auch Anthropic, Building Effective Agents (19. Dezember 2024), abrufbar unter <https://www.anthropic.com/engineering/building-effective-agents>.

5 Bspw. „Generiere Reisepläne inklusive buchbarer Unterkünfte und Transportmittel, wenn ich Reisen in meinen Kalender eintrage.“ oder „Erstelle mir jeden Tag um 18.00 Uhr eine Übersicht, über die wichtigsten Änderungen, die mein Team am jeweiligen Tag an unserer Codebase vorgenommen hat.“

gemacht werden können. Die Zugriffsrechte des Systems können aber noch deutlich weiter gehen: Manche durch OpenClaw nutzbare Funktionen bedürfen zu ihrer Ausführung beispielsweise vollständiger Lese- und Schreibrechte bezogen auf das gesamte System. Sind dem Programm derartige Rechte eingeräumt, kann es theoretisch auf alle auf einem Gerät gespeicherten Daten zugreifen und diese verändern, löschen oder mit anderen Akteuren teilen. Ein solcher KI-Agent kann mit einem Computer also jede Handlung ausführen, die auch ein Mensch (mit außergewöhnlichen Programmierkenntnissen) ausführen könnte. Es handelt sich bei KI-Agenten also um potente und vielseitig einsetzbare Software. In unternehmerischen Kontexten werden sie beispielsweise bereits zur automatisierten Vorratsanalyse und zum Einkauf, in der Vermögensverwaltung, im Kundenkontakt oder auch bei der Bearbeitung von Versicherungsfällen eingesetzt. Individuen können KI-Agenten für private Zwecke, etwa zur Erstellung wetterabhängiger Kochpläne, aber auch für berufliche Zwecke, etwa zur automatischen Beantwortung von E-Mails, einsetzen.

II. Risiken: Von Fehlverhalten, Datenverlust und Cyberangriffen

Diese Fähigkeiten und Einsatzfelder agentischer KI lenken den Blick auf die Risiken der Technologie. Dazu zählt zunächst jegliche Art der Fehlerhaftigkeit der von einem System ausgeführten Aktionen. Im Fall des Autokaufs ist beispielsweise denkbar, dass das System ein falsches oder mehrere Autos kauft, oder einen zu hohen Preis zahlt. Auch bei jeder anderen Art der Verwendung sind aber Fehler denkbar.

Eng damit verknüpft sind Defekte, die zur Beeinträchtigung, Löschung oder Preisgabe privater Daten führen, etwa indem der KI-Agent Datensätze unwiederbringlich löscht, ohne zuvor um Erlaubnis gebeten zu haben, oder private Daten, im Glauben, dies wäre zur Erfüllung der gegebenen Aufgabe nötig, über das Internet an fremde Akteure übermittelt.

Hersteller und Nutzer:innen agentischer KI-Systeme versuchen, diesen Risiken vorzubeugen, indem beispielsweise in (System-) Prompts vorgegeben wird, dass sich das System „strikt an die vorgegebenen Regeln halten soll“ oder „bei Unklarheiten Nachfragen stellen“ soll.[6] Immer wieder gelingt es agentischen KI-Systemen allerdings nicht, solche Vorgaben einzuhalten. Schließlich kreieren KI-Agenten spezifische und teils neuartige Gefahren im Bereich der Cybersecurity. Eine Art dieser Gefahren liegt in sogenannten Prompt Injections. Hier versuchen Angreifer KI-Agenten zur Preisgabe privater Informationen (beispielsweise Passwörter) zu motivieren, indem sie ihnen vorspielen, dies sei zur Erreichung ihres Ziels notwendig. Auch über kompromittierte Tools können aber beispielsweise Angriffe ausgeführt werden. Außerdem sind KI-Agenten in bisherigen Access-and-Identity-Management-Systemen[7] bislang nur selten gut eingebunden; auch dies eröffnet neue Angriffsvektoren.

III. Regulierung I: Dimensionen der Digitalregulierung

Ist für diese Risiken durch bestehende Regulierungsinstrumente hinreichend Vorsorge getroffen? Naheliegend scheint, dass der regulatorische Rahmen der Europäischen KI-Verordnung (KI-VO) hier ausschlaggebend ist. Tatsächlich kennt die KI-VO den Begriff der agentischen KI allerdings nicht. Dennoch enthält die KI-VO einige Pflichten, die für Entwickler und Nutzer agentischer KI besonders relevant sein können. Dazu zählen insbesondere Art. 50 Abs. 1 KI-VO, der vorschreibt, dass KI-Systeme, die direkt mit Menschen interagieren, als solche erkennbar sein müssen, potenziell aber auch Art. 5 Abs. 1 lit. a und b KI-VO, der KI-Systemen verbietet, Menschen zu manipulieren, zu täuschen oder Vulnerabilitäten oder Schutzbedürftigkeiten auszunutzen. Und auch wenn die Qualifikation als agentische KI selbst für die Einstufung eines KI-Systems als Hochrisiko-System keine Rolle spielt – dies beurteilt sich nach dem Verwendungszweck eines Systems – haben gewisse der für Hochrisiko-Systeme geltende Pflichten für agentische KI doch eine besondere Bedeutung. Das gilt insbesondere für Art. 14 KI-VO, der fordert, dass Hochrisiko-KI während der gesamten Zeit ihres Betriebs „von natürlichen Personen wirksam beaufsichtigt werden können“ muss. Das kann bei agentischer KI besondere Probleme bereiten, da diese nicht nur besonders unvorhersehbare Ergebnisse hervorbringen kann, sondern eben auch dafür gedacht ist, in relevanten Aspekten

6 Siehe auch Anthropic, Trustworthy Agents in Practice (9. April 2026), abrufbar unter <https://www.anthropic.com/research/trustworthy-agents>.

7 Unter Access-and-Identity-Management-Systemen versteht man Software, die regelt, wer (welche Person oderwelches Programm) sich in einem Software-System anmelden und autorisieren muss und auf welche Daten und Funktionen eines Systems der Akteur zugreifen darf.

autonom zu handeln. Mechanismen, die absichern, dass der KI-Agent wichtige (beispielsweise irreversible) Handlungen nur nach Einholung einer expliziten Erlaubnis ausführt, können diesen Risiken entgegenwirken, sie aber nicht vollständig beseitigen. Auch bei der Erfüllung der Pflichten zur Transparenz von Hochrisiko-Systemen gem. Art. 13 KI-VO, nach denen Betreiber derartiger Systeme u. a. diese „angemessen interpretieren und betreiben“ können müssen, wie auch der generellen Pflicht zur Risikominimierung gem. Art. 9 KI-VO müssen die Charakteristika und Kapazitäten von agentischen KI-Systemen berücksichtigt werden.

Neben der KI-VO müssen Hersteller und Betreiber von KI-Agenten aber auch noch andere Rechtsbereiche berücksichtigen. Damit ist zum einen das Datenschutzrecht, insbesondere die europäische Datenschutz-Grundverordnung (DSGVO), angesprochen. Hier stellen sich vorwiegend Fragen in den zentralen Bereichen der Zweckbindung und Datenminimierung. Agentische KI lebt nämlich davon, dass ihr Zugriff auf Datenbestände gewährt wird, die aber oftmals nicht für jede ihrer Einsatzmöglichkeiten notwendig sind. Im Ganzen führt ihre Funktionsweise zu einer gewissen Unvorhersehbarkeit der Datenverarbeitung, die nicht unbedingt im Einklang mit den Grundsätzen der DSGVO steht. Auch das Informationssicherheitsrecht spielt aufgrund der bereits angesprochenen spezifischen Cybersicherheitsrisiken eine besondere Rolle. Hier werden u. a. die europäische NIS-2-Richtlinie und deren innerstaatliche Umsetzung sowie der Cyber Resilience Act zum Tragen kommen.

IV. Regulierung II: Haftung und Vertragsschluss

Von besonderer Bedeutung ist auch das Haftungsrecht. Wie bereits bemerkt, kann der Einsatz von KI-Agenten Schäden verursachen, beispielsweise für den:die Nutzer:in des Systems oder für Dritte. Dann drängt sich die Frage auf, wer unter welchen Bedingungen für solche Schäden haftet. Praktisch überlagern sich hier europäisches und nationales Recht: Auf europäischer Ebene sieht die neue EU-Produkthaftungsrichtlinie, die bis Dezember 2026 auch in Deutschland umgesetzt werden muss, vor, dass auch Software und KI-Systeme als Produkte im Sinne des Produkthaftungsrechts zu gelten haben und dass „jede natürliche Person, die einen durch ein fehlerhaftes Produkt verursachten Schaden erleidet …, Anspruch auf Schadensersatz“ hat (Art. 5). Allerdings gelten dabei gewisse Einschränkungen: Ersatzfähig sind nur bestimmte Arten von Schäden, die zwar die „Vernichtung und Beschädigung von Daten“ inkludieren, nicht aber beispielsweise den bloßen Datenverlust. Außerdem sind Schäden an Gegenständen oder Daten, die „ausschließlich für berufliche Zwecke verwendet werden“, ausgeschlossen. Problematisch ist dann natürlich immer auch die Frage, wann ein Produkt beziehungsweise ein KI-System „fehlerhaft“ ist, also „nicht die Sicherheit bietet, die eine Person erwarten darf oder die gemäß Unionsrecht oder nationalem Recht vorgeschrieben ist“.[8] Neben der Produkthaftung kann aber natürlich auch die vertragliche oder deliktische Haftung nach deutschem Recht greifen. Auch hier stellen sich dann komplizierte Fragen nach dem Umfang von Sorgfaltspflichten oder den ersatzfähigen Schäden.

Ähnliche Anpassungen werden sich auch im Vertragsrecht und insbesondere im Recht des Vertragsschlusses vollziehen müssen. Unstrittig können KI-Agenten für natürliche Menschen rechtlich verbindliche Erklärungen übermitteln und also auch Verträge „für sie“ abschließen. Praxis und Justiz werden aber noch klären müssen, ob eine solche rechtsverbindliche Zurechnung in jedem Fall stattfindet oder ob es Situationen gibt, in denen beispielsweise aufgrund der Unvorhersehbarkeit des Handelns des KI-Agenten eine Zurechnung ausscheidet. Außerdem könnten in solchen Situationen auch Anfechtungen oder Ansprüche auf Vertragsanpassung in Betracht kommen.

V. Lässt sich Rechtstreue programmieren?

Je weiter sich KI-Agenten verbreiten und je selbstständiger sie über lange Dauer eigenständig Aufgaben ausführen, desto drängender stellt sich die Frage, wie sichergestellt werden kann, dass sie sich rechtskonform verhalten und keine Schäden anrichten. Eine Antwort auf diese Frage liegt freilich in der Implementierung und Weiterentwicklung von Governance- und sicherheitsbezogenen Best Practices, beispielsweise sichernden (System)-Prompts, beschränkten Zugriffsrechten, angemessener Einbindung von Menschen in Entscheidungsprozesse oder auch sogenannter Kill Switches, also sofort wirksamer Ausschaltknöpfe. Darüber hinaus wird derzeit aber auch an Methoden und Mechanismen gearbeitet, die anwendbares Recht direkt für KI-Agenten zugänglich machen und so ermöglichen sollen, dass KI-Agenten dieses

8 Über diesen Verweis auf das übrige Unionsrecht können also auch Verstöße gegen die KI-VO oder DSGVO Haftung auslösen.

Recht in ihren Aktivitäten berücksichtigen.[9] Ob Mechanismen entwickelt werden können, die zuverlässig eine solche Kongruenz zwischen KI-Agenten und Rechtslage generieren können, ist noch offen. Ansätze gibt es viele.[10] Letztlich handelt es sich bei der Entwicklung rechtskonformer KI-Agenten weniger um ein rein technisches als vielmehr um ein interdisziplinäres Projekt, das Informatik, Rechtswissenschaft und Regulierungspraxis gleichermaßen fordert und bei dem nur durch die Zusammenarbeit dieser verschiedenen Felder überzeugende Ergebnisse zu erwarten sind.

9 Siehe bspw. Cullen O'Keefe et al., Law-following AI: Designing AI agents to obey human laws, Fordham Law Review 94.1 (2025): 57; Noam Kolt et al., Legal Alignment for Safe and Ethical AI, arXiv preprint arXiv:2601.04175 (2026).

10 Bspw. kann man KI-Agenten (schwierige) rechtliche Fragen stellen und beobachten, ob sie diese (nach geltendem Recht) richtig beantworten, oder man kann KI-Systeme trainieren, die besonders gut in der juristischen Analyse sind.

Elektronische Beweismittel ohne Grenzen

Die E-Evidence-Verordnung[1] verschiebt im wahrsten Sinne des Wortes Grenzen bei der Erhebung elektronischer Beweismittel; betrifft sie auch Hochschulen?

Von Nils Bielzer

Am 18. August 2026 werden die Vorschriften der E-Evidence-Verordnung (E-Evidence-VO) verbindlich. Grund genug, sie einmal genauer unter die Lupe zu nehmen. Dazu sollen in diesem Beitrag zentrale Fragen rund um die Anwendbarkeit der Verordnung auf Hochschulen in den Blick genommen werden.

I. Hintergrund

Die E-Evidence-VO hat den Zweck, den grenzüberschreitenden Zugriff auf elektronische Beweismittel in der EU zu erleichtern. Wenn eine Strafverfolgungsbehörde aus einem Staat auf Beweismittel in einem anderen Staat zugreifen will, muss sie (in der Regel über diplomatische Kanäle) ein Rechtshilfeersuchen an den Staat stellen, in dem sich die Beweismittel befinden. Diese Verfahren sind jedoch bisweilen aufwendig, von unsicherem Ausgang und vor allem nicht sonderlich schnell, was gerade bei flüchtigen Daten ein großes Problem darstellt. In der EU gibt es auch deshalb seit 2014[2] die sogenannte Europäische Ermittlungsanordnung,[3] mit der die transnationale Ermittlungsarbeit eine Stufe tiefer auf Behördenebene angesiedelt wird. Strafverfolgungsbehörden aus EU-Staaten können damit ihr jeweiliges Pendant in anderen Mitgliedstaaten zur Erhebung von Beweismitteln auffordern. Neben Dänemark nimmt allerdings auch Irland nicht an dem Verfahren der Europäischen Ermittlungsanordnung teil. Das ist im Bereich elektronischer Beweismittel ein Problem, denn viele große Tech-Unternehmen wie etwa Meta, Google oder Amazon, die über entsprechende Beweismittel verfügen, haben ihre Hauptniederlassung in der EU in Irland. An der E-Evidence-VO nimmt Irland nun aber teil.[4]

Eine direkte Anordnung zur Sicherung oder Herausgabe von Beweismitteln im Ausland war bislang (auch im Rahmen der europäischen Ermittlungsanordnung) nicht möglich. Das soll sich mit der E-Evidence-VO nun zumindest für elektronische Beweismittel[5] ändern. Dabei geht es etwa darum, wem eine gewisse IP-Adresse zugeordnet wurde, wer wann mit wem kommuniziert hat und sogar darum, was der Inhalt der Kommunikation war. Strafverfolgungsbehörden aus EU-Staaten sollen solche Beweismittel direkt bei (bestimmten) in anderen EU-Staaten ansässigen Anbietern elektronischer Kommunikationsdienste und Informationsdienstleistungen anfordern können. Damit sollen die bestehenden, bisweilen aufwendigen und vor allem nicht sonderlich schnellen zwischenstaatlichen Verfahren umgangen werden. Dadurch erhofft man sich insbesondere einen besseren Zugriff auf flüchtige Daten.

---

1 Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren.

2 Die Richtlinie (s. Fn. 3) musste von den Mitgliedstaaten bis 2017 umgesetzt werden.

3 Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen

4 Anders als Dänemark, das Königreich macht auch hier von seinem Opt-out Gebrauch.

5 Art. 3 Nr. 8 E-Evidence-VO definiert „elektronische Beweismittel“ als „Teilnehmerdaten, Verkehrsdaten oder Inhaltsdaten, die zum Zeitpunkt des Erhalts einer Bescheinigung über eine Europäische Herausgabeanordnung (EPOC) oder einer Bescheinigung über eine Europäische Sicherungsanordnung (EPOC-PR) in elektronischer Form von einem Diensteanbieter oder in seinem Auftrag gespeichert werden“.

Die Verordnung bricht dafür mit den klassischen Grundsätzen grenzüberschreitender Ermittlungsarbeit, indem sie Staaten den Erlass rechtsverbindlicher Anordnungen im Ausland ermöglicht. Nach dem Völkerrecht übt in seinem Hoheitsgebiet der jeweilige Staat und grundsätzlich eben nur dieser Staat die Gewalt aus.

Im Rahmen der E-Evidence-VO müssen die Behörden des Vollstreckungsstaats, in dem der adressierte Diensteanbieter sitzt, nur bei der Abfrage von Inhalts- und Verkehrsdaten gem. Art. 8 Abs. 1 E-Evidence-VO überhaupt unterrichtet werden. In diesem Fall kann nach Art. 12 Abs. 1 E-Evidence-VO noch eine Überprüfung durch die zuständige Behörde im Vollstreckungsstaat (in Deutschland die Staatsanwaltschaft[6]) stattfinden und diese eventuell Ablehnungsgründe geltend machen. Allerdings ist die Behörde im Vollstreckungsstaat gem. Art. 8 Abs. 2 E-Evidence-VO nicht zu informieren, wenn hinreichende Gründe für die Annahme bestehen, dass eine Straftat im Anordnungsstaat begangen wurde oder begangen werden wird und die Person, deren Daten angefordert werden, im Anordnungsstaat ansässig ist.

Die Prüfung durch den Vollstreckungsstaat ist also begrenzt. Generell ist der von der Verordnung vorgesehene Rechtsschutz gegen Anordnungen defizitär.[7] Rechtsbehelfe für Betroffene sieht die Verordnung nur im Anordnungsstaat vor, wobei darauf hinzuweisen ist, dass es im Zweifel möglich ist, dass Betroffene nie über die Anordnung informiert werden[8] und so faktisch gar nicht die Möglichkeit haben, Rechtsschutz zu erlangen.

Der deutsche Gesetzgeber hat mit dem Gesetz über die Europäische Herausgabe- und Sicherungsanordnungen zu elektronischen Beweismitteln (EBewMG)[9] Durchsetzungsfragen in Bezug auf die Verordnung geregelt und die flankierende E-Evidence-RL[10] umgesetzt. Die Richtlinie regelt im Wesentlichen die Benennung von Adressaten für Anordnungen nach der E-Evidence-VO seitens der betroffenen Diensteanbieter. Diese sind nach dem deutschen EBewMG beim Bundesamt für Justiz (BfJ) zu benennen.[11] Sie müssen auf der Notification-Platform der EU angemeldet werden, damit ihre Daten an eine Datenbank der EU – die Court Data Base – übermittelt werden können. An diese Adressaten sind die europäischen Herausgabe- und Sicherungsanordnungen zu richten und sie sind auch für deren Bearbeitung zuständig.

Die Benennung hat grundsätzlich bis zum 18. August 2026 zu erfolgen.[12] Bei vorsätzlichen oder fahrlässigen Verstößen gegen die Benennungspflicht drohen Bußgelder bis zu 500.000 Euro.[13] Eine sorgfältige Prüfung minimiert Haftungsrisiken, denn Hochschulen handeln nicht fahrlässig, sofern sie eine sorgfältige juristische Prüfung der Anwendbarkeit vorgenommen und dabei eine vertretbare Rechtsauffassung zugrunde gelegt haben.

II. Anwendbarkeit auf Hochschulen

Auch Hochschulen bieten unter anderem Zugang zum Internet, zu E-Mail-Diensten oder Cloudspeicher an. Es stellt sich also die Frage, ob es sich bei Hochschulen um Diensteanbieter im Sinne der E-Evidence-VO handelt, sodass die Verordnung auf

6 § 11 Abs. 1 EBewMG.

7 Siehe dazu nur: Rath, E-Evidence-Verordung „Deutsches Gesetz verfassungswidrig“ https://anwaltsblatt.anwaltverein.de/de/themen/recht-gesetz/e-evidence-verordnung (zuletzt abgerufen am 29.06.2026); Ambos, schriftliche Stellungnahme im Ausschluss für Recht und Verbraucherschutz des Deutschen Bundestages zu dem Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2023/1544 und zur Durchführung der Verordnung (EU) 2023/1543 über die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel in Strafverfahren innerhalb der Europäischen Union BT-Drucksache 21/3192 vom 9. Januar 2026, Auschuss-Drs. 21(6)49f, abrufbar unter: https://www.bundestag.de/resource/blob/1135990/49f_Stellungnahme_Ambos.pdf.

8 Vgl. Art. 13 Abs. 2 E-Evidence-VO.

9 Gesetz über Europäische Herausgabe- und Sicherungsanordnungen zu elektronischen Beweismitteln (Elektronische-Beweismittel-Umsetzungs-und-Durchführungsgesetz, EBewMG), BGBl. 2026 I Nr. 64 vom 12.03.2026.

10 Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren.

11 § 6 EBewMG.

12 Art. 3 Abs. 6 E-Evidence-RL, § 3 Abs. 5 EBewMG, bei Markteintritt nach dem 18. Februar 2026 beträgt die Frist sechs Monate ab dem jeweiligen Markteintritt.

13 § 18 Abs. 1 Nr. 1, 2 EBewMG.

sie anwendbar wäre. Dabei stellt sich eine Vielzahl an Folgefragen, die überwiegend nicht eindeutig zu beantworten sind. Es existieren bislang weder einschlägige Gerichtsentscheidungen noch adressiert der Gesetzgeber (auch in den begleitenden Gesetzgebungsmaterialien) Hochschulen explizit. Hinzu kommt, dass sich die tatsächlich angebotenen digitalen Dienste zwischen den Hochschulen unterscheiden. Eine abschließende und vor allem allgemeingültige Klärung ist somit zum jetzigen Zeitpunkt nicht möglich. Nach der hier vertretenen Ansicht spricht aber vieles dafür, dass zumindest öffentliche Hochschulen in der Regel nicht von der E-Evidence-VO betroffen sind. Dieser Beitrag stellt wesentliche Fragestellungen hinsichtlich der Anwendbarkeit dar und soll Hochschulen eine Orientierung geben.

Die E-Evidence-VO erfasst Diensteanbieter, die eine der drei in Art. 3 Nr. 3 genannten Kategorien (elektronische Kommunikationsdienste, Internetdomänennamen- und IP-Nummerierungsdienste, Dienste der Informationsgesellschaft) anbieten.

Für Hochschulen kommen konkret die folgenden Dienste infrage:

1. Möglicherweise von Hochschulen erbrachte Dienste

Elektronische Kommunikationsdienste (Art. 3 Nr. 3 lit. a E-Evidence-VO i. V. m. Art. 2 Nr. 4 der European Electronic Communication Code-Richtlinie (EECC-RL)) umfassen vor allem interpersonelle Kommunikationsdienste (z. B. E-Mail-Dienste für Hochschulangehörige) sowie Dienste, die in der Übertragung von Signalen bestehen (z. B. die Bereitstellung von Internetzugängen für Mitglieder der Hochschule). Beide Dienste sind erfasst, sofern sie „gewöhnlich gegen Entgelt“ erbracht werden. Das ist bei öffentlichen Hochschulen fraglich. Internetzugangsdienste (Art. 2 Nr. 4 lit. a EECC-RL[14]) scheiden hingegen in der Regel bereits deshalb aus, weil diese eine öffentliche Zugänglichkeit voraussetzen, was bei Hochschulnetzwerken aufgrund des geschlossenen Benutzerkreises grundsätzlich nicht der Fall ist.[15]

Dienste der Informationsgesellschaft (Art. 3 Nr. 3 lit. c E-Evidence-VO i. V. m. Art. 1 Abs. 1 lit. b RL (EU) 2015/1535) liegen vor, wenn Hochschulen ihren Nutzern Kommunikation ermöglichen (z. B. über E-Mail-Systeme) oder Daten speichern oder verarbeiten (z. B. durch Cloud-Speicherlösungen). Auch diese Dienste müssen allerdings „in der Regel gegen Entgelt erbracht werden“.[16]

Internetdomänennamen- und IP-Nummerierungsdienste (Art. 3 Nr. 3 lit. b E-Evidence-VO) können durchaus von Hochschulen erbracht werden. Das Angebot richtet sich dabei in der Regel nur an Angehörige der eigenen Einrichtung. Aus dem Wortlaut ergibt sich indes nicht, dass die Internetdomänennamen- und IP-Nummerierungsdienste öffentlich zugänglich sein müssen. In den Erwägungsgründen zur E-Evidence-VO wird ausgeführt, diese Diensteanbieter seien „besonders wichtig, wenn es um die Ermittlung von Akteuren geht, die für bösartige oder kompromittierte Websites verantwortlich sind“. Diese Anbieter besitzen Daten, die die Identifizierung einer Person oder eines Rechtsträgers hinter einer für kriminelle Aktivitäten verwendeten Website oder des Opfers einer kriminellen Aktivität ermöglichen könnten.“[17] Für diesen Zweck macht es keinen Unterschied, ob die Kennungen nur an einen begrenzten Personenkreis herausgegeben werden. Es kommt auf die Zuordenbarkeit zu Personen an. Anders als bei den zuvor genannten Diensten besteht hier auch nicht das Erfordernis, dass sie „gewöhnlich“ bzw. „in der Regel gegen Entgelt“ erbracht werden. Dementsprechend muss davon ausgegangen werden, dass Hochschulen – je nach konkretem Angebot – als Anbieter von Internetdomänennamen- und IP-Nummerierungsdiensten im Sinne des Art. 3 Nr. 3 lit. b E-Evidence-VO anzusehen sind. Allerdings wird sich das Angebot dieser Dienste der Hochschulen regelmäßig auf das Gebiet der Bundesrepublik Deutschland beschränken, sodass, wie noch dargelegt wird (s. II. 4.), die Hochschulen trotzdem nicht von der Verordnung betroffen sind.

2. „Gewöhnlich“ bzw. „in der Regel gegen Entgelt“

14 Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation.

15 Ausführlich hierzu John, Der Schutz der Daten im Netz des Access Providers der Wissenschaft, S. 119 ff.

16 Tatbestandsmerkmal hat die gleiche Bedeutung wie die Voraussetzung „gewöhnlich gegen Entgelt erbracht“. Die englische Übersetzung der Rechtsakte verwendet dieselbe Formulierung für beide Begriffe.

17 Erwägungsgrund 28 Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren.

Für die Klärung, ob Hochschulen Anbieter von elektronischen Kommunikationsdiensten (Art. 3 Nr. 3 lit. a E-Evidence-VO i. V. m. Art. 2 Nr. 4 EECC-RL) bzw. Diensten der Informationsgesellschaft (Art. 3 Nr. 3 lit. c E-Evidence-VO i. V. m. Art. 1 Abs. 1 lit. b RL (EU) 2015/1535) sind, ist, wie bereits angeklungen, zentral, ob diese Dienste „gewöhnlich" oder „in der Regel gegen Entgelt" erbracht werden.

Diese Voraussetzung stellt nicht darauf ab, ob im konkreten Fall ein Entgelt verlangt wird. Das wäre bei öffentlichen Hochschulen zu verneinen. Insbesondere handelt es sich bei dem Semesterbeitrag nicht um ein „Entgelt". Stattdessen kommt es darauf an, ob der Dienst typischerweise gegen Entgelt erbracht wird. Entscheidend ist damit die Art des Dienstes. Entscheidend ist die Entgeltlichkeit der Dienste, mit denen der Dienst konkurriert. Wird der überwiegende Anteil dieser Dienste entgeltlich erbracht, sind alle Dienste der Gruppe als „in der Regel entgeltlich" zu betrachten. Es ist also zu fragen, ob die meisten Dienste einer bestimmten Vergleichsgruppe, zu der der infrage stehende Dienst zählt, gegen Entgelt erbracht werden. Ist dies der Fall, liegt die Voraussetzung „gewöhnlich" bzw. „in der Regel gegen Entgelt" für alle Dienste vor.[18]

Entscheidend ist, wie eng bzw. weit man die Vergleichsgruppe zieht.

Man könnte die Vergleichsgruppe weit ziehen, sodass sie auch funktional vergleichbare Dienste umfasst, die nicht von Hochschulen, sondern von kommerziell tätigen Unternehmen erbracht werden. Solche funktional vergleichbaren Dienste (z. B. Cloudspeicher) werden gewöhnlich bzw. in der Regel gegen Entgelt erbracht. Im Fall einer solchen weit gefassten Vergleichsgruppe muss für alle Dienste die Voraussetzung „gewöhnlich" bzw. „in der Regel gegen Entgelt" bejaht werden, sodass dies auch für Dienste von Hochschulen gelten würde.

Allerdings lässt sich die Vergleichsgruppe auch enger ziehen, sodass neben der technischen Funktionsweise zusätzlich auch die konkrete Ausgestaltung und die begleitenden Umstände berücksichtigt werden. Dazu gehören bei Hochschulen etwa, dass das Angebot ausschließlich an Angehörige der eigenen Einrichtung oder eingeschränkte Einsatzzwecke erbracht wird.

Die Voraussetzung „gewöhnlich" bzw. „in der Regel gegen Entgelt" kommt wiederholt in unterschiedlichen Rechtsakten vor und knüpft an Art. 57 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV)[19] an. In Bezug auf die Unterrichtstätigkeit öffentlicher Bildungseinrichtungen hat der Europäische Gerichtshof (EuGH) entschieden, dass diese ihre Leistungen nicht gegen Entgelt anbieten, da der Staat insoweit keine gewinnbringende Tätigkeit aufnehmen wollte, sondern seine sozialen, kulturellen und bildungspolitischen Aufgaben gegenüber seinen Bürger:innen erfüllen will.[20] Anders sieht es nach dem EuGH bei Bildungseinrichtungen aus, die im Wesentlichen durch private Mittel finanziert werden.[21]

Daraus könnte man womöglich ableiten, dass auch im Rahmen des Ausbildungsverhältnisses von staatlichen Hochschulen erbrachte Dienste, die gegenüber dem Ausbildungsverhältnis keine besondere Eigenständigkeit aufweisen, grundsätzlich auch als nicht „gegen Entgelt angeboten" zu betrachten sind. Gleichzeitig kann eine Entgeltlichkeit grundsätzlich auch im Falle öffentlicher Leistungen anzunehmen sein, sofern diese nicht im Wesentlichen durch den allgemeinen Staatshaushalt finanziert werden.[22]
In Bezug auf einen Dienst, bei dem eine „Universität Besuchern auf dem Universitätsgelände kostenlos Zugang zu ihrem WLAN gewährt, ohne eine Vergütung zu erhalten, gleich ob in Form von Zahlungen seitens der Anwender oder in Form von Werbeeinnahmen", stellt der europäische Gesetzgeber in Erwägungsgrund 260 zur EECC-RL beispielhaft klar, dass dieser nicht „in der Regel gegen Entgelt" erbracht wird.[23]

---

18 HK-TTDSG/Assion, 1. Aufl. 2022, TTDSG § 3 Rn. 75.

19 Art. 57 AEUV definiert „Dienstleistungen" im Rahmen der europäischen Primärverträge.

20 EuGH, Urt. v. 11.09.2007, Az. C-76/05, Rn. 39.; EuGH, Urt. v. 27.09.1988, Az. C 263/86, Rn. 18.

21 EuGH, Urt. v. 11.09.2007, Az. C-76/05, Rn. 40 ff.; EuGH, Urt. v. 07.12.1993, Az. C-109/92 Rn. 17.

22 M.w.N. Armin/Rothkegel in Taeger/Gabel, DSGVO – BDSG – TDDG, 5. Auflage 2026, Art. 4 DSGVO Rn. 508.

23 Ludwigs EU-WirtschaftsR-HdB/Micklitz/Rott, 63. EL Mai 2025, § 53 Rn. 214; Spindler/Schmitz/Spindler, 2. Aufl. 2018, TMG § 5 Rn. 7, 8; Entgeltlichkeit in Bezug auf von Hochschulen bereitgestellte Videokonferenzsysteme verneinend, Roßnagel, NJW 2023, 400 (402); fragend in Bezug auf den Entwurf für die E-Commerce-RL hingegen Hoeren, MMR 1999, 192.

In der rechtswissenschaftlichen Literatur finden sich Stimmen, die jeweils im Kontext eines spezifischen Rechtsakts annehmen, dass von Hochschulen angebotene Dienste nicht „gewöhnlich" bzw. „in der Regel gegen Entgelt" erbracht werden.

Auch ihren Angestellten stellen Hochschulen etwa E-Mail-Accounts und Zugang zum Internet bereit. Die Frage, ob Arbeitgeber:innen, die ihren Arbeitnehmer:innen Dienste zur Verfügung stellen, Diensteanbieter sind bzw. sein können, ist seit vielen Jahren umstritten.[24] Dies ist wohl zu verneinen. In dieser Beziehung ist davon auszugehen, dass Arbeitnehmer:innen grundsätzlich kein Entgelt für die Leistungen der Arbeitgeber:innen entrichten.[25]

Zusammenfassend lässt sich sagen, dass gewichtige Gründe dafür sprechen, dass die von öffentlichen Hochschulen bereitgestellten Dienste gegenüber ihren Studierenden, ihren Angestellten und zum Teil auch gegenüber Dritten nicht „gewöhnlich" bzw. „in der Regel gegen Entgelt" angeboten werden.

Allerdings bestehen zu der Frage, soweit ersichtlich, keine Gerichtsentscheidungen. Die vom Oberverwaltungsgericht (OVG) Münster in einem Vorabentscheidungsverfahren dem EuGH vorgelegte Frage zur Auslegung des Tatbestandsmerkmals „gewöhnlich gegen Entgelt", insbesondere wie weit die Vergleichsgruppe zu ziehen ist, ließ der EuGH leider unbeantwortet.[26] Eine Einordnung geht dementsprechend mit einer erhöhten Rechtsunsicherheit einher.

3. Private Hochschulen

Bei privaten Hochschulen besteht der Unterschied, dass etwaige angebotene Dienste hier in ein grundsätzlich „gegen Entgelt" ausgestaltetes Verhältnis eingebettet sind,[27] sodass man durchaus zu dem Ergebnis kommen kann, dass auch von ihnen gegenüber Studierenden erbrachte Dienste „gewöhnlich" bzw. „in der Regel gegen Entgelt" angeboten werden.

In Bezug auf die Erbringung von Diensten für Mitarbeiter:innen bestehen aber bei privaten Hochschulen keine Besonderheiten.

4. Ausnahme wegen Anbietens von Diensten in nur einem Mitgliedstaat

Die E-Evidence-VO findet nur Anwendung, wenn einer der genannten Dienste in der Europäischen Union angeboten wird. Dabei liegt der Verordnung grundsätzlich ein weites Verständnis des Begriffs des „Anbietens" zugrunde. Gemäß Art. 3 Nr. 4 lit. a E-Evidence-VO genügt hierfür, dass die Hochschule es natürlichen oder juristischen Personen ermöglicht, die Dienste in Anspruch zu nehmen. Darüber hinaus bedarf es gemäß Art. 3 Nr. 4 lit. b E-Evidence-VO einer „wesentlichen Verbindung" zu dem jeweiligen Mitgliedstaat. Diese besteht laut der Verordnung jedenfalls dann, wenn eine Niederlassung in dem Mitgliedstaat besteht. Das ist bei Hochschulen in aller Regel der Fall.

Sofern man nur den Wortlaut der Verordnung zugrunde legt, könnte der Eindruck entstehen, dass auch Anbieter betroffen sind, deren Angebot auf das Gebiet des Staates beschränkt ist, in dem sie niedergelassen sind. Die Verordnung spricht in Art. 3 Nr. 4 ausdrücklich von „einem" (lit. a) bzw. „einem oder mehreren Mitgliedstaaten" (lit. b).

Allerdings können gem. Art. 7 Abs. 1 E-Evidence-VO Europäische Herausgabe- und Sicherungsanordnungen nur an eine „benannte Niederlassung" (Art. 3 Nr. 6 E-Evidence-VO) bzw. einen „Vertreter" (Art. 3 Nr. 7 E-Evidence-VO) gerichtet werden. Die Pflicht zur Benennung einer „benannten Niederlassung" bzw. zur Bestellung eines „Vertreters" bestimmt sich nach der E-Evidence-RL (vgl. I.). Gem. Art. 1 Abs. 5 S. 2 der E-Evidence-RL gilt diese „nicht für Diensteanbieter, die im Hoheitsgebiet nur eines Mitgliedstaats niedergelassen sind und ihre Dienste nur im Hoheitsgebiet dieses Mitgliedstaats anbieten". Auch aus § 3 Abs. 2 des EBewMG ergibt sich im Umkehrschluss, dass Diensteanbieter, die über eine oder mehrere Niederlassungen ausschließlich auf dem Gebiet der Bundesrepublik Deutschland verfügen und ihre Dienste nicht zusätzlich oder alternativ in einem weiteren Mitgliedstaat anbieten, keinen Adressaten benennen müssen.

Anbieter, die nur in einem Mitgliedstaat niedergelassen sind und nur dort ihre Dienste anbieten, benennen demnach keine „benannten Niederlassungen" oder „Vertreter", sodass es an

---

24 Aufarbeitung des Streitstands konkret für die E-Evidence-VO Weiß/Pradel, CCZ 2024, 102; vgl. in Bezug auf Internetnutzung auch Thiessen, All work no play …, DFN-Infobrief Recht 11/2019.

25 Weiß/Pradel, CCZ 2024, 102.

26 EuGH, Urt. v. 13.06.2019, Az. C-193/18, s. insb. Vorlagefrage 3. c).

27 Vgl. Fn. 20, 21.

dem von Art. 7 Abs. 1 E-Evidence-VO (und indirekt auch von Art. 7 Abs. 2 E-Evidence-VO) vorausgesetzten Adressaten für Anordnungen nach der E-Evidence-VO fehlt. Entsprechende Anbieter sind somit nicht bloß von der Anmeldung befreit, vielmehr findet die Verordnung nach dieser Auslegung unter Heranziehung der Rechtsvorschriften und der begleitenden Gesetzesmaterialien auch generell keine Anwendung auf sie.

Diese Ausnahme ist etwas versteckt in der Systematik der E-Evidence-Rechtsakte. In der rechtswissenschaftlichen Literatur wurde ihr, soweit ersichtlich, noch keine Aufmerksamkeit geschenkt. Das für die Verwaltung der Adressaten zuständige Bundesamt für Justiz (BfJ) weist aber in dem Dokument „Prüfung – bin ich Diensteanbieter?“ auf sie hin.[28]

Doch wie wird bestimmt, ob Anbieter ihre Dienste „nur im Hoheitsgebiet dieses Mitgliedstaats erbringen“? Zur Beantwortung dieser Frage kann auf die Erwägungsgründe der E-Evidence-VO und der E-Evidence-RL zurückgegriffen werden, die sich mit der Frage des „Anbieters von Diensten in der Europäischen Union“ auseinandersetzen.[29] Demnach sind eine Vielzahl von Kriterien zu berücksichtigen. Dazu gehört etwa eine erhebliche Zahl von Nutzer:innen in einem oder mehreren Mitgliedstaaten.[30] Auch die Ausrichtung, also ein Abzielen des Angebots auf einen oder mehrere Mitgliedstaaten, ist von Bedeutung. Ob eine solche Ausrichtung vorliegt, ist anhand aller relevanten Umstände, einschließlich Faktoren wie der Verwendung einer in dem betreffenden Mitgliedstaat gebräuchlichen Sprache oder Währung bzw. der Möglichkeit, Waren oder Dienstleistungen zu bestellen, zu bestimmen.[31] Die Verfügbarkeit einer App im jeweiligen nationalen App-Store oder die Schaltung lokaler Werbung kann ebenfalls Berücksichtigung finden.[32] Gleichzeitig wird in den Erwägungsgründen klargestellt, dass die Erbringung einer Dienstleistung zur bloßen Einhaltung des Diskriminierungsverbots der Geoblocking-VO[33,34] allein nicht ausreicht, um eine Ausrichtung auf ein bestimmtes Gebiet innerhalb der Union anzunehmen.[35]

Noch wichtiger ist wohl der Hinweis darauf, dass die bloße Zugänglichkeit einer Online-Schnittstelle in der Union, beispielsweise die Zugänglichkeit einer Website oder einer E-Mail-Adresse oder anderer Kontaktdaten eines Diensteanbieters oder eines Vermittlers, für sich genommen nicht als ausreichend angesehen

---

28 Bundesamt für Justiz, Prüfung - bin ich Diensteanbieter? abrufbar unter: https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Evidence/Pruefungsschema.pdf?__blob=publicationFile&v=4.

29 Erwägungsgrund 30 Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren; Erwägungsgrund 12 Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren (, jeweils der letzte Satz).

30 ebd.

31 ebd.

32 ebd.

33 Verordnung (EU) 2018/302 des Europäischen Parlaments und des Rates vom 28. Februar 2018 über Maßnahmen gegen ungerechtfertigtes Geoblocking und andere Formen der Diskriminierung aufgrund der Staatsangehörigkeit, des Wohnsitzes oder des Ortes der Niederlassung des Kunden innerhalb des Binnenmarkts und zur Änderung der Verordnungen (EG) Nr. 2006/2004 und (EU) 2017/2394 sowie der Richtlinie 2009/22/EG.

34 Die Geoblocking-VO verbietet es Anbietern innerhalb der Europäischen Union, Kund:innen aufgrund ihrer Staatsangehörigkeit, ihres Wohnsitzes oder ihres Standorts beim Zugriff auf Websites, beim Kauf von Waren oder bei der Inanspruchnahme von Dienstleistungen ungerechtfertigt zu diskriminieren

35 Erwägungsgrund 30 Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren; Erwägungsgrund 12 Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren.

werden kann, um festzustellen, ob ein Diensteanbieter Dienste im Sinne dieser Verordnung in der Union anbietet.[36]

Die von Hochschulen (möglicherweise) angebotenen Dienste werden regelmäßig nur in einem Mitgliedstaat eine erhebliche Anzahl an Nutzer:innen haben. Zwar gibt es auch Hochschulen, die im Ausland für sich werben. Die Werbung bezieht sich in der Regel aber auf ein Studium im Land der Niederlassung, sodass die Dienste dann in der Regel ebendort erbracht werden. Gerade auch im Hinblick darauf, dass etwa die reine Zugänglichkeit aus weiteren Mitgliedstaaten eben nicht ausreichen soll, wird bei vielen Hochschulen eher keine Ausrichtung auf einen anderen Mitgliedstaat vorliegen. Gleichzeitig sind durchaus Fälle denkbar, in denen Hochschulen Dienste in einem anderen Mitgliedstaat als dem ihrer Niederlassung erbringen. So beispielsweise bei einem grenzüberschreitenden Fernstudium, bei dem einer oder mehrere der genannten Dienste erbracht werden. Ebenso können Dienste im Ausland im Rahmen von grenzüberschreitenden Kooperationen angeboten werden. Eine umfassende Prüfung des konkreten Angebots der jeweiligen Hochschule unter den genannten Gesichtspunkten bleibt somit unerlässlich.

III. Fazit

Bei der E-Evidence-VO handelt es sich um einen echten Paradigmenwechsel im grenzüberschreitenden Beweismittelrecht. Die Frage, ob Hochschulen ihrem Anwendungsbereich unterfallen, lässt sich nicht abschließend und vor allem nicht allgemeingültig beantworten. Unterm Strich werden wohl viele von Hochschulen angebotene Dienste aus den in diesem Beitrag dargestellten Gründen eher nicht in den Anwendungsbereich der E-Evidence-VO fallen. Das entbindet Hochschulen jedoch nicht davon, das von ihnen konkret angebotene Diensteportfolio im Hinblick auf die Anwendbarkeit der E-Evidence-VO zu überprüfen. In Bezug auf die aufgeworfenen Fragen ist zu hoffen, dass der nun anlaufende Vollzug für mehr Klarheit sorgt.

36 Erwägungsgrund 29 Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren; Erwägungsgrund 11 Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren.

Cyberresilienz auch für Hochschulen?

Die EU legt mit dem Cyber Resilience Act (CRA)[1] einheitliche Cybersicherheitsanforderungen für Hard- und Software fest

Von Philipp Schöbel

Auf EU-Ebene regelten bereits vor der Verabschiedung des CRA mehrere Rechtsakte einzelne Aspekte der Cybersicherheit.[2] Allerdings bestanden keine unmittelbar verbindlichen Anforderungen an die Sicherheit von Produkten mit digitalen Elementen (ErwG 3 CRA). Der CRA[3] gilt für eine Reihe unterschiedlicher vernetzter Produkte: von einfachen Verbraucher:innenprodukten bis zu Industriesoftware.[4] Die neuen Regelungen sind auch für Hochschulen und Forschungseinrichtungen relevant.

I. Produkte mit digitalen Elementen

Der CRA gilt für Produkte mit digitalen Elementen und legt grundlegende Cybersicherheitsanforderungen für diese fest (Art. 1 CRA). Ein Produkt mit digitalen Elementen bezieht sich sowohl auf Software als auch auf Hardware (Art. 3 Nr. 1 CRA). Software wird als der Teil eines elektronischen Informationssystems, der aus Computercode besteht, definiert (Art. 3 Nr. 4 CRA). Hardware ist hingegen nach der Legaldefinition ein physisches elektronisches Informationssystem, das digitale Daten verarbeiten, speichern oder übertragen kann oder Teile eines solchen Systems (Art. 3 Nr. 5 CRA). Der sachliche Anwendungsbereich ist durch den bestimmungsgemäßen Zweck und die vernünftigerweise vorhersehbare Verwendung etwas eingeschränkt. Denn Zweck und Verwendung müssen eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz umfassen (Art. 2 Abs. 1 CRA). Dies dürfte jedoch faktisch auf eine Vielzahl von Hard- oder Software zutreffen. Der sachliche Anwendungsbereich des CRA ist demnach grundsätzlich weit gefasst und erstreckt sich auch etwa auf vernetzte Verbrauchergeräte, IT-Hardware und „reine“ Software.[5] Auch ein Campusmanagementsystem (CMS) dürfte regelmäßig vom Anwendungsbereich des CRA erfasst sein. Weitere Beispiele im Hochschulbereich sind etwa Software für die Raumbuchung von Hörsälen oder Seminarräumen, Identity-Management-Systeme oder auch Bibliotheksverwaltungssoftware.

II. Ausnahmen vom Anwendungsbereich

Einige Produktarten sind vom Anwendungsbereich des CRA ausgenommen. Ausnahmen gelten etwa für die

1 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, 20.11.2024.

2 Zur Darstellung des EU-Cybersicherheitsrechts: Schöbel, Cybersicherheit an Hochschulen in Europa – eine Übersicht, DFN-Infobrief Recht 9/2025, 11-14.

3 Zum Entwurf des CRA siehe: Palenberg, Cyber Angriff ade mit dem CRA-E?, DFN-Infobrief Recht 9/2023, S. 2-5.

4 Vgl. BSI, Cyber Resilience Act, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html (alle Quellen zuletzt abgerufen am 05.06.2026).

5 Teichmann, NJW 2025, 2577, 2578.

Medizinprodukteverordnung,[6] die In-vitro-Diagnostika-Verordnung[7] oder die Verordnung (EU) 2019/2144[8] (Art. 2 Abs. 2 CRA). Ebenfalls ausgenommen sind Produkte, die unter die EU-Schiffsausrüstungsrichtlinie fallen (Art. 2 Abs. 4 CRA). Die aufgezählten Produktsicherheitsrechtsakte legen bereits hohe Anforderungen an die Cybersicherheit fest, weshalb der CRA keine Sicherheitsstandards für diese Produkte festlegt.[9] Für Hochschulen dürften diese Ausnahmen in der Regel nicht relevant sein. Demnach bleibt es für den Hochschulsektor grundsätzlich bei einem sehr weiten Anwendungsbereich des CRA.

III. Adressaten

Der CRA adressiert eine Reihe von Akteur:innen. Unterschiedliche Pflichten gelten etwa für Hersteller:innen (Art. 13, 14 CRA), für Einführer:innen, für Händler:innen (Art. 20 CRA) oder für Verwalter:innen quelloffener Software (Art. 24 CRA). Nicht adressiert sind Betreiber:innen von Software. Hersteller:in meint zum einen die Person, die ein Produkt mit digitalen Elementen entweder selbst entwickelt oder herstellt oder die solche Produkte konzipieren, entwickeln oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet (Art. 3 Nr. 13 CRA). Es ist unerheblich, ob dies gegen Bezahlung, zur Monetarisierung oder unentgeltlich erfolgt (Art. 3 Nr. 13 CRA). Ein Beispiel für das Vermarkten von Software unter eigenem Namen ist etwa, wenn auf der Startseite des Programms der Produktname auf die Hersteller:inn hindeutet.[10] Dafür ist es grundsätzlich unerheblich, wie sich die Akteur:innen in der Wertschöpfungskette vertraglich geeinigt haben.[11]

Der Begriff des/der Einführer:in meint die Person, die das Produkt unter dem Namen oder der Marke einer außerhalb der Union ansässigen oder niedergelassenen natürlichen oder juristischen Person in der Union in den Verkehr bringt (Art. 3 Nr. 16 CRA). Als Händler:in gilt die Person, die das Produkt ohne Änderung seiner Eigenschaften auf dem Unionsmarkt bereitstellt, soweit sie nicht schon Hersteller:in oder Einführer:in ist (Art. 3 Nr. 17 CRA). Bereitstellen meint die entgeltliche oder unentgeltliche Abgabe eines Produkts zum Vertrieb oder zur Verwendung auf dem EU-Markt im Rahmen einer Geschäftstätigkeit (Art. 3 Nr. 22 CRA). Unklar ist, ob die Bereitstellung von Software an Studierende auch eine Abgabe zur Verwendung auf dem EU-Markt darstellt. Eine Abgabe zur Verwendung liegt vor, „wenn das Produkt mit digitalen Elementen zu dem vom/von der Hersteller:in definierten Verwendungszweck eingesetzt wird."[12] Ein Produkt wird auf dem EU-Markt bereitgestellt, wenn die Endnutzung ebenfalls innerhalb der EU erfolgt.[13] Auch eine Hochschule, die Studierenden Zugang zu einer Software gewährt, könnte demnach im Einzelfallals Händler:in im Sinne des CRA angesehen werden.

In bestimmten Fällen können Personen, die nicht Hersteller:innen des Produkts sind, dennoch als Hersteller:in nach dem CRA gelten. Diese rechtliche Kategorie der „Quasi-Hersteller:in" findet sich

6 Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, ABl. L 117 S. 1, 2019 L 117 S. 9.

7 Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission, ABl. L 117 S. 176, ber. ABl. 2019 L 117 S. 11.

8 Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern, zur Änderung der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnungen (EG) Nr. 78/2009, (EG) Nr. 79/2009 und (EG) Nr. 661/2009 des Europäischen Parlaments und des Rates sowie der Verordnungen (EG) Nr. 631/2009, (EU) Nr. 406/2010, (EU) Nr. 672/2010, (EU) Nr. 1003/2010, (EU) Nr. 1005/2010, (EU) Nr. 1008/2010, (EU) Nr. 1009/2010, (EU) Nr. 19/2011, (EU) Nr. 109/2011, (EU) Nr. 458/2011, (EU) Nr. 65/2012, (EU) Nr. 130/2012, (EU) Nr. 347/2012, (EU) Nr. 351/2012, (EU) Nr. 1230/2012 und (EU) 2015/166 der Kommission, ABl. L 325 S. 1.

9 Teichmann, NJW 2025, 2577, 2578; Schöttle, MMR 2024, 741, 743.

10 Mehnert, in: NK-CRA, 1. Aufl. 2026, CRA Art. 3 Rn. 82.

11 Mehnert, in: NK-CRA, 1. Aufl. 2026, CRA Art. 3 Rn. 82.

12 Poncza, in: NK-CRA, 1. Aufl. 2026, CRA Art. 3 Rn. 137.

13 Poncza, in: NK-CRA, 1. Aufl. 2026, CRA Art. 3 Rn. 140.

auch in anderen Rechtsakten, etwa in Art. 25 der Verordnung über künstliche Intelligenz (KI-VO).[14] Händler:innen und Einführer:innen gelten als Hersteller:innen, wenn sie das Produkt unter eigenem Namen oder eigener Marke in den Verkehr bringen (Art. 21 Var. 1 CRA). Darüber hinaus gelten sie als Hersteller:innen, wenn sie eine wesentliche Änderung an einem bereits in den Verkehr gebrachten Produkt mit digitalen Elementen vornehmen (Art. 21 Var. 2 CRA). Eine ähnliche Regelung gilt für Personen, die nicht bereits Händler:in oder Einführer:in sind. Diese gelten als Hersteller:in, wenn sie eine wesentliche Änderung an dem Produkt vornehmen und dieses Produkt auf dem Markt bereitstellen (Art. 22 Abs. 1 CRA). Eine wesentliche Änderung im Sinne des CRA meint eine Änderung, die sich auf die Konformität des Produkts auswirkt oder zu einer Änderung des bestimmungsgemäßen Zwecks führt (Art. 3 Nr. 30 CRA). Die Änderung muss nach dem Inverkehrbringen erfolgen. Der bestimmungsgemäße Zweck richtet sich nach dem Willen des/der Hersteller:in und ergibt sich aus besonderen Nutzungsumständen und Nutzungsbedingungen entsprechend den Angaben der Hersteller:innen in der Gebrauchsanleitung, im Werbe- oder Verkaufsmaterial und in Erklärungen sowie in der technischen Dokumentation (Art. 3 Nr. 23 CRA). Hochschulen, die etwa Software zu einem anderen Zweck einsetzen als zu dem, für den das Produkt von der/dem Hersteller:in geprüft wurde, könnten daher gegebenenfalls auch als Händler:in gelten. Dies gilt jedoch nur, wenn sie das Produkt auf dem Markt bereitstellen.

Verwalter:innen quelloffener Software können nur juristische Personen sein (Art. 3 Nr. 14 CRA). Diese dürfen nicht mit dem/der Hersteller:in identisch sein. Sie müssen das Ziel haben, die Entwicklung spezifischer Produkte mit digitalen Elementen, die als freie und quelloffene Software gelten und für kommerzielle Tätigkeiten bestimmt sind, systematisch und nachhaltig zu unterstützen. Zudem müssen sie auch die Brauchbarkeit dieser Produkte sicherstellen. Freie und quelloffene Software ist eine Software, deren Quellcode offen geteilt wird und die im Rahmen einer kostenlosen Open-Source-Lizenz zur Verfügung gestellt wird, die alle Rechte vorsieht, um sie frei zugänglich, nutzbar, veränderbar und weiterverteilbar zu machen (Art. 3 Nr. 48 CRA). Inwieweit auch Hochschulen oder Forschungseinrichtungen Verwalter:innen quelloffener Software sein können, hängt von den Umständen des Einzelfalls ab.

IV. Pflichten der Hersteller:innen

Hersteller:innen müssen eine Reihe von Pflichten erfüllen, die jedoch an einen Unterstützungszeitraum für das Produkt gekoppelt sind und somit nicht ewig gelten.[15] Der Unterstützungszeitraum ist der Zeitraum, in dem der/die Hersteller:in sicherstellen muss, dass die Schwachstellen des Produkts mit digitalen Elementen wirksam und im Einklang mit den grundlegenden Cybersicherheitsanforderungen des CRA behandelt werden (Art. 3 Nr. 20 CRA). Der/die Hersteller:in hat diesen so festzulegen, dass er die Dauer der voraussichtlichen Nutzung des Produkts widerspiegelt (Art. 13 Abs. 8 UAbs. 2 S. 1 CRA).
Zunächst müssen Hersteller:innen dafür sorgen, dass die Produkte, die sie in Verkehr bringen, gemäß den grundlegenden Cybersicherheitsanforderungen des CRA konzipiert, entwickelt und hergestellt worden sind (Art. 13 Abs. 1 CRA). Diese grundlegenden Cybersicherheitsanforderungen sind in Anhang I des CRA festgelegt. Weiterhin haben sie die Cybersicherheitsrisiken ihrer Produkte kontinuierlich zu bewerten (Art. 13 Abs. 2 CRA). Auch sind Hersteller:innen dazu verpflichtet, ein kontinuierliches Schwachstellenmanagement durchzuführen (Art. 13 Abs. 8 UAbs. 1 CRA).[16] Hersteller:innen müssen ausgenutzte Schwachstellen in ihren Produkten zudem an die ENISA[17] melden (Art. 14 Abs. 1 S. 1 CRA). Für diese Meldungen richtet die ENISA eine einheitliche Meldeplattform ein (Art. 16 Abs. 1 S. 1 CRA).

V. Pflichten der Händler:innen

Händler:innen treffen eine Reihe von formellen Prüfpflichten: So müssen sie etwa überprüfen, ob der/die Hersteller:in die Kennzeichnungen und Dokumentationen dem Produkt entsprechend beigefügt hat.[18] Darüber hinaus unterliegen sie

14 Siehe zum Quasi-Anbieter nach Art. 25 KI-VO: Schöbel, Was sind Quasi-Anbieter von KI-Systemen?, DFN-Infobrief Recht 1/2026, 11-14.

15 Paschke/Fellenberg, EuDIR 2025, 198, 200.

16 Vgl. Paschke/Fellenberg, EuDIR 2025, 198, 200.

17 Die ENISA ist die Agentur der Europäischen Union für Cybersicherheit. Sie wurde im Jahr 2004 gegründet und hat ihren Sitz in Attiki, Griechenland.

18 Schneider, in: BeckOK Produktrecht, 6. Ed. 15.4.2026, Cyberresilienz-VO Art. 20 Rn. 1.

Informationspflichten. Soweit die/der Händler:in feststellt, dass ein Produkt ein erhebliches Cybersicherheitsrisiko birgt, muss sie/er etwa unverzüglich den/die Hersteller:in und die Marktüberwachungsbehörde unterrichten (Art. 20 Abs. 3 S. 2 CRA). Ein erhebliches Cybersicherheitsrisiko liegt vor, wenn aufgrund der technischen Merkmale des Risikos davon auszugehen ist, dass es mit hoher Wahrscheinlichkeit zu einem Sicherheitsvorfall führen wird, der schwerwiegende negative Auswirkungen haben und erhebliche materielle oder immaterielle Verluste oder Störungen verursachen könnte (Art. 3 Nr. 38 CRA). Sobald die Händler:innen von einer Schwachstelle in einem Produkt mit digitalen Elementen Kenntnis erhalten, müssen sie den/die Hersteller:in unverzüglich über diese Schwachstelle informieren (Art. 20 Abs. 4 UAbs. 2 S. 1 CRA).

VI. Pflichten der Verwalter:innen quelloffener Software

Die Verwalter:innen quelloffener Software müssen auf überprüfbare Weise eine Cybersicherheitsstrategie entwickeln und dokumentieren (Art. 24 Abs. 1 Hs. 1 CRA). Diese Pflicht dient der Entwicklung eines sicheren Produkts mit digitalen Elementen sowie einem wirksamen Umgang mit Schwachstellen durch die Entwickler:innen dieses Produkts (Art. 24 Abs. 1 Hs. 2 CRA). Diese Strategie fördert auch die freiwillige Meldung von Schwachstellen durch die Entwickler:innen (Art. 24 Abs. 1 S. 2 CRA). Die Pflicht zur Meldung von Cybersicherheitsvorfällen betrifft teilweise auch die Verwalter:innen quelloffener Software (Art. 24 Abs. 3 i. V. m. Art. 14 CRA).[19]

VII. Hochrisiko-KI-Systeme

Der CRA ist ebenfalls relevant für die Anforderungen an die Cybersicherheit von Hochrisiko-KI-Systemen nach der KI-VO. Diese ist wiederum auch für den Hochschulbereich relevant,[20] denn KI-Systeme im Bereich von Lehre und Hochschulverwaltung können Hochrisiko-KI-Systeme im Sinne der KI-VO darstellen (Art. 6 Abs. 2 i. V. m. Anhang III Nr. 3, 4 KI-VO).[21] Diese Hochrisiko-KI-Systeme müssen so konzipiert werden, dass sie ein angemessenes Maß an Cybersicherheit gewährleisten (Art. 15 Abs. 1 KI-VO). Werden die Anforderungen des CRA eingehalten, gelten auch die Anforderungen an die Cybersicherheit nach der KI-VO als erfüllt (Art. 12 Abs. 1 CRA). Durch diese Regelung wird der CRA in die KI-VO integriert.[22] Soweit Hochschulen Anbieter:innen von Hochrisiko-KI-Systemen sind, sollten sie daher auch die Bestimmungen des CRA beachten.

VIII. Ausblick

Für Hochschulen und Forschungseinrichtungen bedeutet der CRA zum einen, dass sie prüfen müssen, ob sie den Pflichten des CRA unterliegen. Je nach Fallkonstellation können sie etwa grundsätzlich Hersteller:innen oder Händler:innen im Sinne des CRA sein. Zum anderen profitieren sie aber auch von den Pflichten des CRA. Auch Hochschulen und Forschungseinrichtungen sind weitestgehend darauf angewiesen, dass die von ihnen verwendeten IT-Systeme reibungslos funktionieren. Cybersicherheitsvorfälle können die Arbeit in Lehre, Forschung und Verwaltung teils immens beeinträchtigen oder gar vollständig lahmlegen. Die Verpflichtungen der Hersteller:innen von Hard- und Software nach dem CRA können zu einem verbesserten Cybersicherheitsniveau in der EU beitragen. Daher schützen die neuen Regelungen mittelbar auch den Betrieb der deutschen Wissenschaftslandschaft.

Der CRA wird ab dem 11. Dezember 2027 in der gesamten EU gelten (Art. 71 Abs. 2 UAbs. 1 CRA). Einzelne Pflichten gelten jedoch schon früher. Die Pflicht der Hersteller:inen, ausgenutzte Cybersicherheitsschwachstellen zu melden (Art. 14 CRA), gilt etwa bereits ab dem 11. September 2026 (Art. 71 Abs. 2 UAbs. 2 CRA). Zeit, dass sich auch der Wissenschaftssektor mit den neuen Regelungen auseinandersetzt.

---

19 Vgl. Paschke/Fellenberg, EuDIR 2025, 198, 202.

20 Siehe etwa: Rennert, One Kiss is all it takes, DFN-Infobiref Recht 1/2023; Schöbel, AI Act – Licht der Europäischen Union, DFN-Infobrief Recht 12/2024, S. 7-12; Der AI Act und die Wissenschaft, DFN-Infobrief Recht 2/2025, S. 2-7; KI-Modelle made in Europe?, DFN-Infobrief Recht 4/2025, S. 14-20; Friedl, Mit digitalen Wasserzeichen zu klareren Informationsökosystemen?, DFN-Infobrief Recht 5/2026, S. 2-5.

21 Siehe dazu Schöbel: KI-Folgenabschätzung für Hochschulen?, DFN-Infobrief Recht 7/2026, S. 8 f.

22 Hofmann, in: NK-CRA, 1. Aufl. 2026, CRA Art. 12 Rn. 3.

DFN Infobrief-Recht-Aktuell

- ## EU-Recht/Datenschutzrecht: Der Europäische Datenschutzausschuss (EDSA) beschließt neue Leitlinien zur Anonymisierung personenbezogener Daten

Mit den am 8. Juli 2026 veröffentlichten neuen Leitlinien zur Anonymisierung hat der EDSA den Begriff anonymer Daten unter Berücksichtigung der Rechtsprechung des Europäischen Gerichtshofs (EuGH), insbesondere des Urteils des EuGH vom 4. September 2025, konkretisiert. Danach sind Daten anonym, wenn sie sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen. Die Leitlinien sollen zudem einen praktischen Rahmen bieten, um festzustellen, ob eine Anonymisierung erfolgreich durchgeführt wurde. Dabei sind drei Kriterien maßgeblich, um zu beurteilen, ob Daten anonym sind: keine Aufzeichnungsisolation, keine Verknüpfung und keine Schlussfolgerung.

Hier erhalten Sie den Link zur Leitlinie des EDSA (alle Links dieser Seite wurden zuletzt am 22.07.2026 abgerufen):
https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202602_anonymisation_v1_en_0.pdf

- ## Informationsfreiheitsrecht: Die Informationsfreiheitsbeauftragten kritisieren die Pläne der Bundesregierung, das Informationsfreiheitsgesetz massiv einzuschränken

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) stellt sich gegen die Pläne der Bundesregierung, das Informationsfreiheitsgesetz deutlich einzuschränken. Die Bundesregierung plant, den voraussetzungslosen Zugang zu Verwaltungsinformationen einzuschränken. Nach den veröffentlichten Plänen des Koalitionsausschusses soll der Auskunftsanspruch künftig von einem berechtigten Interesse abhängen und nur dann zum Tragen kommen, wenn keine anderen Informationsrechte bestehen. Darüber hinaus sollen nur natürliche Personen mit Wohnsitz in Deutschland sowie Deutsche oder Unionsbürger Anträge stellen dürfen. Vollständige Bereiche wie die Kritische Infrastruktur oder die wissenschaftliche Forschung sollen pauschal vom Anwendungsbereich ausgenommen werden. Die IFK kritisiert, dass insbesondere das Erfordernis eines berechtigten Interesses die Abwendung vom Prinzip des voraussetzungslosen Anspruchs auf Zugang zu amtlichen Informationen bedeuten würde.

Hier erhalten Sie den Link zur Pressemitteilung der IFK:
https://www.lda.brandenburg.de/lda/de/service/presseinformationen/details-presse/~06-07-2026-konferenz-der-informationsfreiheitsbeauftragten-informationsfreiheitsbeauftragte-kritisie

- ## Urheberrecht: Urteil des EuGH zur Gemeinfreiheit und Geoblocking

Der EuGH hat am 9. Juli 2026 entschieden, dass ein Werk, das in bestimmten Mitgliedstaaten gemeinfrei geworden ist, auf einer Internetseite veröffentlicht werden darf, auch wenn es in einem anderen Mitgliedstaat weiterhin urheberrechtlich geschützt ist. Voraussetzung dafür ist, dass eine wirksame technische Maßnahme wie Geoblocking eingesetzt wird, um den Zugriff auf diese Seite für Internetnutzer der Mitgliedstaaten, in denen das Werk geschützt ist, zu sperren. Hintergrund des Rechtsstreits ist die gerichtliche beantragte Unterlassung der Verbreitung der Manuskripte von Anne Frank durch den Anne Frank Fonds. Die Manuskripte sind in den Niederlanden urheberrechtlich geschützt, in anderen Ländern sind sie gemeinfrei geworden.

Hier erhalten Sie den Link zur Entscheidung:
https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62024CJ0788

Kurzbeitrag: Googeln verboten?

Warum Arbeitgeber Bewerber:innen nicht ohne Weiteres im Internet recherchieren dürfen

Von Elena Sacoph

Der Fall ging bis vor das Bundesarbeitsgericht: Ein Bewerber forderte Schadensersatz wegen Verstößen gegen die Datenschutz-Grundverordnung (DSGVO),[1] weil an einem Stellenbesetzungsverfahren beteiligte Mitarbeitende einer Universität eine Internetrecherche über ihn durchgeführt hatten. Zu Recht, entschied das Bundesarbeitsgericht (BAG).[2] Die Universität musste 1.000 Euro Schadensersatz zahlen.

I. Entscheidung

Es begann wie ein gewöhnliches Bewerbungsverfahren: Eine Universität suchte im Rahmen einer Elternzeitvertretung eine Volljuristin bzw. einen Volljuristen für ihr Justiziariat. Nach einem Vorstellungsgespräch erhielt der Bewerber eine Absage mit der Begründung, dass sich die Universität für eine andere Person entschieden habe, die das Anforderungsprofil für die Stelle besser erfülle. So weit, so unspektakulär.

Doch der Bewerber, Volljurist und Fachanwalt für Arbeitsrecht, wollte es nicht darauf beruhen lassen und verlangte gegenüber der Universität Auskunft nach Art. 15 DSGVO. Daraufhin übersandte die Universität ihm eine Kopie des Auswahlvermerks, der der Auswahlentscheidung zugrunde lag.

Anhand des Auswahlvermerks war ersichtlich, dass die Universität den Bewerber im Internet recherchiert hatte und dabei aus öffentlich zugänglichen Quellen von einer gerichtlichen, aber noch nicht rechtskräftigen Verurteilung erfahren hatte. Der Bewerber war erstinstanzlich wegen Betrugs und versuchten Betrugs zu einer Freiheitsstrafe von einem Jahr und vier Monaten auf Bewährung verurteilt worden. Der Vorwurf lautete, er habe mehrfach fingierte Bewerbungen eingereicht, um potenzielle Arbeitgeber anschließend wegen angeblicher Diskriminierung zur Zahlung von Entschädigungen nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) zu veranlassen. Hiergegen hatte der Bewerber Revision beim Bundesgerichtshof (BGH) eingelegt, worüber zum Zeitpunkt der Internetrecherche aber noch nicht entschieden worden war. Aus dem Auswahlvermerk war weiterhin ersichtlich, dass die Universität diese Informationen ausdrücklich in ihre Entscheidung, genauer in ihre Absage, einbezogen hatte.

Daraufhin klagte der Bewerber und machte gleich mehrere Ansprüche geltend: Bei einer nicht rechtskräftigen Verurteilung gelte für ihn die Unschuldsvermutung, und allein deswegen stünde seiner Eignung nichts entgegen. Des Weiteren berief er sich auf Art. 33 Abs. 2 Grundgesetz (GG), wonach das Recht auf eine ermessens- und beurteilungsfehlerfreie Einbeziehung in die Stellenauswahl für öffentliche Ämter gilt.[3] Er war der Ansicht, der am besten qualifizierte Bewerber gewesen zu sein, und sah durch die Absage sein grundgesetzliches Recht verletzt. Schließlich

1 VO 2016/679.

2 BAG 05.06.2025 8 AZR 117/24. Online abrufbar unter: https://www.bundesarbeitsgericht.de/wp-content/uploads/2025/09/8-AZR-117-24.pdf (alle Links des Beitrags wurden zuletzt am 18.06.2026 abgerufen).

3 Art. 33 Abs. 2 GG lautet: „Jeder Deutsche hat nach seiner Eignung, Befähigung und fachlichen Leistung gleichen Zugang zu jedem öffentlichen Amte." Öffentliche Ämter im Sinne des Art. 33 Abs. 2 GG sind nicht nur Beamtenstellen, sondern auch Stellen, die ein Arbeitgeber des öffentlichen Dienstes mit Arbeitnehmer:innen zu besetzen beabsichtigt, vgl. BVerfG, 1 BvR 2317/15, 08.11.2016.

habe die Universität außerdem gleich gegen mehrere Bestimmungen der DSGVO verstoßen, indem sie personenbezogene Daten „hinter seinem Rücken“ aus dem Internet erhoben und ihn nicht darüber informiert habe.

Durch mehrere Instanzen ging es bis zum Bundesarbeitsgericht. Dieses bestätigte schließlich das Urteil des Landesarbeitsgerichts. Dem Kläger seien weder Schadensersatzansprüche aus dem Bürgerlichen Gesetzbuch (BGB) zuzusprechen, noch sei Art. 33 Abs. 2 GG verletzt. Begründete Zweifel zum Zeitpunkt der Auswahlentscheidung rechtfertigen die Ablehnung eines Bewerbers. Ein laufendes Strafverfahren kann, je nach Tatvorwurf und ausgeschriebener Tätigkeit, ein ausreichender Grund für solche Zweifel sein. Die Unschuldsvermutung steht dem nicht zwingend entgegen. Sie bindet unmittelbar nur die Gerichte, schließt aber nicht etwa aus, dass einem Beschuldigten aus einem anhängigen Strafverfahren nicht-strafende Nachteile entstehen dürfen, so das Bundesarbeitsgericht.

Das Landesarbeitsgericht hatte dem Kläger einen immateriellen Schadensersatz in Höhe von 1.000 Euro aus Art. 82 Abs. 1 DSGVO zugesprochen, weil die Universität ihn nicht über ihre Internetrecherche informiert hatte. Vor dem Bundesarbeitsgericht blieb es dabei. Fazit: Kein Schadensersatz für den entgangenen Job, aber 1.000 Euro wegen eines DSGVO-Verstoßes.[4]

II. Hintergrund: 1.000 Euro für Kontrollverlust

Doch was bedeutet dies? Darf man Bewerber:innen etwa nicht googeln? Zunächst ist festzuhalten: Auch öffentlich auffindbare Informationen im Internet bleiben personenbezogene Daten im Sinne der DSGVO. Daher stellt eine Internetrecherche auch eine Datenverarbeitung nach Art. 4 Nr. 2 DSGVO dar. Aus einer solchen Datenverarbeitung erwächst in jedem Fall die Pflicht, die recherchierte Person gemäß Art. 14 DSGVO zu informieren.

Ob schon die Recherche selbst datenschutzwidrig war, ließ das Gericht allerdings offen. Aber: Die Recherche darf jedenfalls nicht im Geheimen oder, wie es der Kläger formulierte, „hinter dem Rücken“ der betroffenen Person stattfinden. Die Informationspflichten aus Art. 14 DSGVO sind einzuhalten. Wird die Person nicht informiert, kann sie, wie im geschilderten Fall, einen Schadensersatzanspruch aus Art. 82 Abs. 1 DSGVO geltend machen. Doch worin besteht hier eigentlich der „Schaden“ und wie wird er bemessen?

Der Kläger machte geltend, dass ihm ein Schaden dadurch entstanden sei, dass er nicht über die Verarbeitung seiner personenbezogenen Daten informiert wurde und ihm so auch die Möglichkeit verwehrt blieb, dazu Stellung zu nehmen.

Zunächst ist festzuhalten, dass nicht jeder Verstoß gegen die DSGVO automatisch einen Schadensersatzanspruch nach sich zieht. Für einen Anspruch aus Art. 82 Abs. 1 DSGVO müssen drei Voraussetzungen vorliegen: Es braucht einen DSGVO-Verstoß, einen tatsächlichen Schaden und schließlich einen Kausalzusammenhang zwischen Verstoß und Schaden. Tatsächlich kann bereits der „Verlust der Kontrolle“ über die eigenen Daten einen Schaden im Sinne der DSGVO darstellen.[5] In seiner Klage bezifferte der abgelehnte Bewerber den Schaden auf 5.000 Euro.

Das Landesarbeitsgericht bemaß den Schaden hingegen mit 1.000 Euro. Das Bundesarbeitsgericht bestätigte diese Entscheidung und verwies auf die Ausführungen des Europäischen Gerichtshofs (EuGH). Dessen Rechtsprechung habe geklärt, dass der in Art. 82 Abs. 1 DSGVO geregelte Schadensersatzanspruch ausschließlich eine ausgleichende und keine strafende Funktion hat.[6] Es kommt also allein darauf an, welchen (immateriellen) Schaden die betroffene Person tatsächlich erfahren hat. Die Höhe des Schadensersatzanspruchs bemisst sich dann nach dem konkret

4 Ein Kurzbeitrag zu einem ähnlich gelagerten Fall findet sich hier: Tech, Wie gewonnen, so zerronnen, DFN-Infobrief Recht 04/2024.

5 Vgl. EuGH 14.12.2023 C-340/21. Hier stellte der EuGH unter Verweis auf den ersten Satz des 85. Erwägungsgrunds der DSGVO klar, dass der Unionsgesetzgeber unter den Begriff „Schaden“ insbesondere auch den bloßen „Verlust der Kontrolle“ über die eigenen Daten infolge eines Verstoßes gegen die DSGVO fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil der Personen erfolgt sein sollte. Online abrufbar unter:
https://infocuria.curia.europa.eu/tabs/document?source=document&text=&docid=280623&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1.

6 Vgl. EuGH v. 04.10.2024 C-507/23. Online abrufbar unter:
https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62023CJ0507.

erlittenen Verlust. Ein bestimmter Grad an „Erheblichkeit“ ist keine Voraussetzung.[7]

Außerdem machte das Bundesarbeitsgericht in seiner Entscheidung klar, dass sich die Bemessung des Schadensersatzes nicht automatisch erhöht, wenn mehrere Verstöße gegen die DSGVO vorliegen. Solange sich diese auf denselben Verarbeitungsvorgang beziehen, ist auch hier allein der vom Betroffenen konkret erlittene Schaden entscheidend. So erachtete das Gericht 1.000 Euro als ausreichend, um den immateriellen Schaden auszugleichen.

III. Praxis: Recherche nur mit Rechtsgrundlage und Transparenz

Für die Praxis der Bewerber:innenauswahl bedeutet das: Vorsicht ist besser als Nachsicht. Das Urteil des Bundesarbeitsgerichts sowie die Rechtsprechung des EuGH machen deutlich, dass bereits der bloße Kontrollverlust über die eigenen Daten im Zusammenhang mit einem DSGVO-Verstoß einen Schadensersatzanspruch begründen kann.[8]

Zwar haben die Gerichte nicht abschließend entschieden, ob Internetrecherchen im Rahmen eines Stellenbesetzungsverfahrens unzulässig sind oder nicht. Klar ist jedoch, dass sie in jedem Fall Informationspflichten im Sinne des Art. 14 DSGVO begründen. Sollte es zu einer Internetrecherche kommen, ist diese daher sauber zu dokumentieren, auf öffentlich zugängliche Quellen zu beschränken und auf das erforderliche Maß zu reduzieren. Die recherchierte Person sollte umgehend informiert werden. Insbesondere wenn die Suchergebnisse für die Stellenbesetzung relevant werden könnten, sollte der betroffenen Person Gelegenheit zur Stellungnahme gegeben werden, bevor eine Entscheidung fällt.

---

7 Vgl. EuGH v. 04.05.2023 C-300/21. Online abrufbar unter: https://infocuria.curia.europa.eu/tabs/document?source=document&text=&docid=273284&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=4941430. Siehe hierzu auch Voget, Nicht (un)erheblich, DFN-Infobrief Recht 07/2023.

8 Zu datenschutzrechtlichen Schadensersatzansprüchen siehe auch: Müller, Schaden oder kein Schaden, das ist hier die Frage, DFN-Infobrief Recht 03/2023.

Impressum

Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz.

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 Humboldt-Universität Berlin.

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

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

Tel. (030) 838-66754

E-Mail: recht@dfn.de

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