„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

# infobrief recht DFN

9/2025
September 2025


## Vor dem Betreiber sind alle Daten gleich

Netzneutralität hat wieder Konjunktur – was besagt die hierzu geltende europäische Verordnung und kommt ein Digital Networks Act?

## Es DMAert so langsam

Die Europäische Kommission verhängt die ersten Bußgelder gegen Gatekeeper wegen Verstößen gegen den Digital Markets Act (DMA)

## Cybersicherheit an Hochschulen in Europa – eine Übersicht

Das europäische Cybersicherheitsrecht hat sich in den letzten Jahren rasant weiterentwickelt – Zeit für einen hochschulspezifischen Überblick

## Kurzbeitrag: Gut gemeint, doch schlecht gemacht: Bundesverfassungsgericht kippt Postdoc-Paragraf für Berliner Hochschulen

Das Land Berlin scheitert mit dem Versuch, Hochschulen zu verpflichten, Post-docs Dauerstellen anzubieten

# Vor dem Betreiber sind alle Daten gleich

## Netzneutralität hat wieder Konjunktur – was besagt die hierzu geltende europäische Verordnung und kommt ein Digital Networks Act?

*Von Nikolaus von Bernuth, Berlin*

Die Netzneutralität ist ein wesentliches Strukturmerkmal des offenen Internets. Die Europäische Union (EU) erließ im Jahr 2015 eine Verordnung, die die Netzneutralität garantiert. Einige Jahre war es verhältnismäßig ruhig um das Thema. Doch jüngst kam es vermehrt zu Rechtsunsicherheit und Streitigkeiten über die Reichweite der Netzneutralität. Auch auf politischer Ebene gibt es neue Bestrebungen: Die EU plant einen Digital Networks Act, der auch Einschränkungen der Netzneutralität zur Folge haben könnte.

## I. Hintergrund

Das Internet ist ein wesentlicher Teil der digitalen Infrastruktur unserer Gesellschaft. Es dient den Menschen dazu, sich mit Informationen zu versorgen, Geschäfte zu tätigen oder zu kommunizieren. Auch für Hochschulen und Forschungseinrichtungen ist das Internet elementar. Forschung erfolgt heutzutage digital und vernetzt – auch die Lehre ist spätestens seit der Corona-Pandemie nicht mehr rein analog denkbar. Das Internet ist daher für nahezu alle Lebensbereiche kritische Infrastruktur.

Der Zugang zum Internet sollte daher grundsätzlich nach fairen und diskriminierungsfreien Bedingungen möglich sein. Dies gilt sowohl für die Endnutzer:innen als auch für die Inhalteanbieter, die etwa eine Website betreiben.[1] Welche Daten von wem angeboten oder angefragt werden, sollte für den Transport über die Infrastruktur irrelevant sein. Nur so kann ein freies und offenes Internet bestehen.

Diese Überlegungen werden unter dem Stichwort Netzneutralität verhandelt, das durch den Rechtswissenschaftler Tim Wu geprägt wurde.[2] Ab Beginn der 2010er-Jahre wurde in Deutschland und Europa intensiv über die Netzneutralität und ihre Absicherung diskutiert. Der Bundestag setzte im Jahr 2010 eine Enquete-Kommission „Internet und digitale Gesellschaft“ ein, die sich auch dem Thema Netzneutralität widmen sollte. Die Enquete-Kommission diskutierte kontrovers, konnte sich aber nicht auf konkrete Handlungsempfehlungen einigen.[3] Im Jahr 2015 erließ schließlich der europäische Gesetzgeber die Telecom-Single-Market-Verordnung (TSM-VO), auch bekannt als Open Internet Regulation oder Netzneutralitätsverordnung.[4]

In den vergangenen Jahren ist erneut Bewegung in die Debatte gekommen. Zum einen stellen sich Kosten- und Verteilungsfragen immer drängender. Peering und Interconnection-Praktiken werfen zudem Fragen zur Reichweite der Netzneutralität auf. Und nicht zuletzt plant der europäische Gesetzgeber einen Digital Networks Act, in dessen Rahmen die Netzneutralität - zur Überraschung vieler - auf den Prüfstand kommen könnte. Anlass genug, das Thema grundlegend zu beleuchten.

1 Ob die Netzneutralität nach geltendem europäischem Recht auch letztere schützt, ist aber umstritten.

2 Wu, Network Neutrality, Broadband Discrimination, Journal on Telecommunications & High Technology Law 2003, Volume 2, 141-176.

3 Vgl. Schlussbericht der Enquete-Kommission „Internet und digitale Gesellschaft“ v. 5.4.2013, Bundestags-Drucksache. 17/12550, S. 13.

4 Verordnung (EU) 2015/2120 vom 25. November 2015.

## II. Die Telecom-Single-Market-Verordnung

Die Art. 1 bis 6 TSM-VO regeln auf europäischer Ebene die Netzneutralität. Als Verordnungsvorschriften gelten sie unmittelbar in allen Mitgliedstaaten. Ziel der Normen ist die „Wahrung der gleichberechtigten und nichtdiskriminierenden Behandlung des Verkehrs bei der Bereitstellung von Internetzugangsdiensten und der damit verbundenen Rechte der Endnutzer“ (Art. 1 Abs. 1 TSM- VO).

### 1. Das Prinzip der Netzneutralität

Der Wesenskern der Netzneutralität ist in Art. 3 Abs. 3 TSM -VO festgehalten. Internetzugangsdienste (also Netzbetreiber) müssen den gesamten Internetverkehr gleichbehandeln - also ohne Diskriminierung, Beschränkung oder Störung. Diese Gleichbehandlung muss unabhängig von der sendenden und empfangenden Person, den abgerufenen oder verbreiteten Inhalten, den genutzten oder bereitgestellten Anwendungen oder Diensten sowie den verwendeten Endgeräten gewährleistet sein. Jedes einzelne Datenpaket muss entsprechend der Systemauslastung bestmöglich transportiert werden (sog. Best-Effort-Prinzip).

Die Bundesnetzagentur formuliert: „Netzneutralität liegt vor, wenn der gesamte Datenverkehr in einem Netz gleich (das heißt neutral) behandelt wird - unabhängig von Inhalt, Anwendung, Dienst, Absender und Empfänger.“[5] In Anlehnung an den Allgemeinen Gleichheitssatz des Grundgesetzes (Art. 3 Abs. 1 GG)[6] lässt sich sagen: Vor dem Betreiber sind alle Daten gleich.

### 2. Verkehrsmanagement

Diese grundsätzliche Gleichbehandlung des Datenverkehrs darf nur in Ausnahmefällen eingeschränkt werden. Damit nimmt der Gesetzgeber insbesondere auf sog. Verkehrsmanagementmaßnahmen Rücksicht (Art. 3 Abs. 3 UAbs. 2, 3 TSM-VO). Dies können Maßnahmen sein, die erforderlich sind, um den reibungslosen Betrieb des Netzes sicherzustellen, drohende Netzüberlastungen zu verhindern oder die Dienstqualität in sonstiger Weise sicherzustellen. Auch diese Verkehrsmanagementmaßnahmen müssen ihrerseits aber angemessen, transparent, nichtdiskriminierend und verhältnismäßig sein. Dies erfordert primär, dass die Maßnahmen nicht auf kommerziellen Erwägungen, sondern objektiven technischen Gründen beruhen.

### 3. Transparenz

Der Grundsatz der Netzneutralität soll durch korrespondierende Transparenzpflichten begleitet werden. Ein Vertrag über die Bereitstellung eines Internetzugangs muss nach Art. 4 TSM-VO bestimmte Angaben enthalten. Dazu gehören Angaben über die Verkehrsmanagementmaßnahmen sowie Volumen- oder Geschwindigkeitsbeschränkungen (wie sie im Mobilfunk noch üblich sind). Zudem müssen auch Informationen zu den normalerweise verfügbaren, den maximalen sowie den beworbenen Geschwindigkeiten der Netzverbindung enthalten sein.

### 4. Aufsicht und Durchsetzung

Trotz der Kürze der Verordnung regelt die TSM-VO auch die Aufsicht und Durchsetzung der Regeln zur Netzneutralität. Zuständig für die Aufsicht sind insbesondere die nationalen Regulierungsbehörden, Art. 5 Abs. 1 TSM-VO. In Deutschland ist dies die Bundesnetzagentur mit Sitz in Bonn, § 191 Telekommunikationsgesetz (TKG). Die Bundesnetzagentur kann, nachdem sie einen Verstoß gegen die Netzneutralität festgestellt hat, das betroffene Unternehmen zur Stellungnahme auffordern und Abhilfe des rechtswidrigen Verhaltens verlangen, § 202 Abs. 1 TKG. Kommt das Unternehmen dem nicht nach, kann die Bundesnetzagentur die erforderlichen Maßnahmen anordnen und diese mit Zwangsgeldern von bis zu 10 Mio. Euro durchsetzen, § 202 Abs. 2, Abs. 5 TKG.

Auf europäischer Ebene wurde daneben im Jahr 2010 das Gremium europäischer Regulierungsstellen für elektronische Kommunikation (BEREC) gegründet.[7] Es hat seinen Sitz in Riga, Lettland. Das Gremium soll unabhängig, unparteiisch und transparent die nationalen Behörden koordinieren und beraten.

---

5 Bundesnetzagentur, https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/Schutz/Netzneutralitaet/start.html.

6 Art. 3 Abs. 1 GG lautet: „Alle Menschen sind vor dem Gesetz gleich“.

7 Begründung durch Verordnung (EG) Nr. 1211/2009; nun auf Grundlage von Verordnung (EU) 2018/1971. Im Deutschen auch abgekürzt als GEREK.

Besonders zentral sind die Leitlinien des BEREC. Um die einheitliche Anwendung der Regeln zur Netzneutralität sicherzustellen, erarbeitet BEREC präzisierende Leitlinien, Art. 5 Abs. 3 TSM-VO. Diese Leitlinien haben für das Verständnis der Netzneutralität eine prägende Bedeutung.

## III. Problemfelder

Die Netzneutralität als prägendes Strukturmerkmal des Internets wird grundlegend kaum infrage gestellt. Dennoch kam über ihre Bedeutung und insbesondere ihre Reichweite zuletzt immer wieder Streit auf.

### 1. Wer zahlt für die Infrastruktur?

Eine Herausforderung für die Netzneutralität ist insbesondere die ungleich verteilte Nutzungslast der Netze. Ein Bericht der großen europäischen Netzbetreiber aus dem Jahr 2022 zeigte: Etwa 57 % der Internetnutzung gehen auf sechs der größten Anbieter digitaler Dienste zurück (Google, Facebook, Netflix, Apple, Amazon, Microsoft). Differenziert nach Nutzungsart machen Videodienste, Social Media und Gaming 70 % der weltweiten Internetnutzung aus.[8] Dieser Wert dürfte angesichts der zunehmend erfolgreichen videobasierten Dienste noch gestiegen sein.

Nun stellen diese großen digitalen Dienste ihre Inhalte über das Internet bereit – um die dafür nötige Infrastruktur kümmern sich hingegen andere. Netzbetreiber bauen die Netze aus und bieten Endkunden ihre Dienstleistungen (Zugang zum Internet) an. Insbesondere der kontinuierliche Netzausbau, der mit den steigenden Datenmengen Schritt halten muss, verursacht erhebliche Kosten. Um die Verteilung dieser Kosten wird immer wieder gestritten. Netzbetreiber argumentieren, dass gerade die großen Dienste mit erheblichem Datenaufkommen proportional an den Kosten von Netzausbau und Netzbetrieb beteiligt werden müssen.

Doch hier kommt das Prinzip der Netzneutralität ins Spiel. Dieses könnte einer solchen Forderung nach Kostenbeteiligung gerade entgegenstehen. Wenn es sich etabliert, dass bestimmte große Anbieter spezifische Vereinbarungen und Kooperationen mit den Netzbetreibern eingehen, könnte sich im Internet eine Zweiklassengesellschaft herausbilden und die Netzneutralität untergraben werden. So befürchtet es ein zivilgesellschaftliches Bündnis, das jüngst eine Beschwerde bei der Bundesnetzagentur eingereicht hat.[9]

### 2. Peering und die Interconnection-Ebene

Damit ist eine Praxis angesprochen, die bereits absolut marktüblich ist. Über sogenanntes Peering bzw. Interconnection schließen Unternehmen und Netzbetreiber ihre Netze häufig über gesonderte Verbindungen zusammen. Dies hat den Vorteil, dass die Daten schneller fließen und nicht über die allgemeinen Verteilwege des Internets laufen müssen. Große Videostreamingdienste laufen so verlässlich flüssig. Im Ausgangspunkt bringen solche Peerings allen Beteiligten Vorteile: Die Unternehmen arbeiten reibungsloser zusammen, das Gesamtnetz wird entlastet und die Nutzenden erhalten am Ende eine bessere Dienstleistung.

Probleme können aber daraus entstehen, dass die Netzbetreiber teils Geld für diese Peering-Verbindungen verlangen.[10] Der Vorwurf lautet, dass diese schnellen und vorteilhaften Netzzusammenschlüsse nur kommerziellen, finanzkräftigen Akteuren offenstehen. Dies gehe zulasten des Gesamtnetzes, das nicht im gleichen Maße optimiert werde. Wer also etwa nur eine kleine, eventuell sogar nicht kommerzielle Website betreibe, komme nicht in den Genuss der effizienteren Netzverbindung. Dieser Zustand stehe aber gerade im Kontrast zum Wesensgehalt der Netzneutralität, nach dem alle Daten gleichzubehandeln seien.

Die Netzbetreiber stehen auf dem Standpunkt, dass das Peering notwendig sei und nur Gewinner hervorbringe. Dass für das Peering Geld verlangt werde, hänge mit der sehr ungleichen Verteilung der Nutzungslast zusammen. Es sei ein legitimes Mittel, Geld bei denen abzuschöpfen, die am meisten von den

8 Axon, Europe's internet ecosystem: socio-economic benefits of a fairer balance between tech giants and telecom operators, 05/2022, S. 12-13, abrufbar hier: https://www.telefonica.com/en/wp-content/uploads/sites/5/2022/05/20220425_Axon-Full-Report-Final-corrected.pdf (alle Links dieses Beitrags zuletzt abgerufen am 20.07.2025).

9 Vgl. dazu https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-netzneutralität.

10 Vgl. hierzu https://www.netzbremse.de.

Netzverbindungen profitieren. Rechtlich besteht Unklarheit darüber, ob die Regeln zur Netzneutralität auch das Peering erfassen. Nach einer Ansicht, die sich insbesondere auf den Gesetzeswortlaut und die Schutzrichtung der TSM-VO stützt, sei das Peering gerade nicht erfasst. Die Netzneutralität schütze nur den Bereich der Bereitstellung von Internetzugangsdiensten gegenüber den Endnutzer:innen.[11] Nach anderer Ansicht, die auch der einflussreiche BEREC in einer Leitlinie vertritt, können Interconnection-Vereinbarungen dann in Konflikt mit der Netzneutralität treten, wenn sie Auswirkungen auf die Endnutzer:innen haben.[12] Hierauf stützt sich auch die bereits angesprochene Beschwerde aus der Zivilgesellschaft. [13]Diese Unklarheit wird nun in einem ersten Schritt durch die Bundesnetzagentur zu beantworten sein, in der Folge könnte sie auch die Gerichte beschäftigen.

### 3. Zero-Rating

In einem anderen Rechtsstreit bekam der Europäische Gerichtshof (EuGH) bereits die Gelegenheit, die Netzneutralität näher zu konturieren. Gegenstand des Streits waren sog. Zero-Rating-Pakete, die von verschiedenen Mobilfunkanbietern angeboten wurden.[14] Im Kern bedeutete dies, dass ausgewählte Datenströme - etwa das Videostreaming von verpartnerten Inhalteanbietern - nicht auf die Volumenbeschränkungen angerechnet wurden.

In drei parallelen Urteilen befand der EuGH am 2. September 2021, dass dieses Angebot gegen das Prinzip der Netzneutralität in Art. 3 Abs. 3 TSM-VO verstoße.[15] Das Zero-Rating führe nach Ansicht des EuGH zu einer Ungleichbehandlung des Datenverkehrs aufgrund kommerzieller Erwägungen. Bereits ein Jahr zuvor hatte der EuGH ein ähnlich gelagertes Angebot untersagt.[16] Diese Rechtsprechung hat schließlich dazu geführt, dass derartige Angebote vom Markt genommen wurden.

## IV. Ausblick: Digital Networks Act

Die EU plant nun eine Reform des europäischen Rechtsrahmens für den Telekommunikationsmarkt. Im Geiste der vergangenen Jahre (Digital Services Act, Digital Markets Act) will der europäische Gesetzgeber eine Verordnung mit dem Titel „Digital Networks Act“ erarbeiten. Die Verordnung soll den geltenden Regulierungsrahmen vereinheitlichen, Rechtsunsicherheiten beseitigen und für mehr Innovation sorgen.

Einen Entwurf hat die dafür zuständige Europäische Kommission bislang nicht vorgelegt. Sie hat allerdings erste Eckpunkte veröffentlicht, zu denen eine öffentliche Konsultation eingeholt wurde.[17] Aus den ersten Angaben der Kommission geht hervor, dass im Digital Networks Act bestimmte Erleichterungen für sog. Spezialdienste geplant sind. Das könnten etwa bezahlte Überholspuren sein, die eine besonders schnelle Internetverbindung für bestimmte Services versprechen. Es wird argumentiert, dass nur so gewisse Innovationen wirksam vorangebracht werden könnten – etwa in der Telemedizin. Verbraucherschützer befürchten hingegen, dass die Netzneutralität als Innovationshemmnis gebrandmarkt und so insgesamt zur Verhandlungsmasse werden könnte.[18]

Doch ob die bisherigen Regelungen der TSM-VO unklar und daher reformbedürftig sowie innovationshemmend sind, wird sehr unterschiedlich beurteilt. Sollte die Netzneutralität tatsächlich

---

11 So, insbesondere Koenig/Veidt, MMR 2025, 83, 84 m. w. N.

12 BEREC Guidelines, Guideline 6, 2022, abrufbar unter: https://www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-the-implementation-of-the-open-internet-regulation-0.

13 Die Beschwerde findet sich unter https://www.netzbremse.de.

14 Siehe dazu bereits ausführlich Gielen, Liberté, Égalité, StreamOn adé, DFN-Infobrief Recht 11/2021; Gielen, Dream On, Telekom!, DFN-Infobrief Recht 09/2019.

15 EuGH, Urteile vom 02.09. 2021, Az. C-34/20, C-854/19, C-5/20. Näher dazu Gielen, Liberté, Égalité, StreamOn adé, DFN-Infobrief Recht 11/2021.

16 EuGH, Urt. v. 15.9.2020, Az. C-807/18, C-39/19.

17 Zum Verfahrensstand: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14709-Digital-Networks-Act_en.

18 Zum Hintergrund Rudl, netzpolitik.org, 27.06.2025, https://netzpolitik.org/2025/bremse-oder-motor-eu-kommission-stellt-netzneutralitaet-zur-debatte/.

neu geregelt werden, könnte der Gesetzgebungsprozess zur nächsten symbolbeladenen Diskussion um das offene und freie Internet werden.

# Es DMAert so langsam

## Die Europäische Kommission verhängt die ersten Bußgelder gegen Gatekeeper wegen Verstößen gegen den Digital Markets Act (DMA)

*Von Ole-Christian Tech, Münstern*

Der (DMA) hat zuletzt vor allem politisch hohe Wellen geschlagen. Das neue europäische Instrument zur Bändigung der Marktmacht ausländischer Big-Tech-Konzerne wurde in den jüngsten Zollstreitigkeiten mit den USA sogar Teil der Verhandlungsmasse. Grund dafür dürfte auch die - zumindest implizite - Zielsetzung des Rechtsakts sein, ein nichttarifäres Handelshemmnis für die digitalen Dienste großer, überwiegend US-amerikanischer Technologiekonzerne zu schaffen.

## I. Zielsetzung und Struktur des DMA

Digitalmärkte neigen aufgrund starker Netzwerkeffekte oftmals zur Monopolisierung.[1] Trotz des Wettbewerbsrechts auf europäischer Ebene und in den Mitgliedstaaten ist es bislang nicht gelungen, den Wettbewerb in der digitalen Ökonomie effektiv zu regulieren. Um dieses Versäumnis zu kompensieren, hat die Europäische Union den Digital Markets Act als ex-ante-Regulierungsansatz entworfen.[2] Dieser ist als europäische Verordnung seit dem 2. Mai 2023 in allen Mitgliedstaaten anwendbar.

Der DMA hat das Ziel, bestreitbare und faire Märkte im digitalen Sektor durch harmonisierte Vorschriften für die gesamte Union zu gewährleisten, Art. 1 Abs. 1 DMA. So soll ein fairer Wettbewerb gefördert werden. Der Fokus der Regelung liegt auf den großen Plattformunternehmen, den sogenannten Gatekeepern, die durch ihre marktbeherrschende Stellung eine besondere Position einnehmen.

Der Begriff der Bestreitbarkeit zielt darauf ab, Märkte für Wettbewerber zu öffnen und offenzuhalten, indem Markteintritts- und Expansionshindernisse abgebaut und der Zugang zu essenziellen Inputfaktoren ermöglicht wird.[3] Ziel ist eine höhere Effizienz der Märkte durch Wettbewerb.

Fairness bezieht sich dagegen auf das Gleichgewicht der Rechte und Pflichten von gewerblichen Nutzern und Gatekeepern. Gatekeeper sollen aufgrund ihrer Stellung keine „unverhältnismäßigen" Vorteile zulasten ihrer gewerblichen Nutzer erzielen. Hierbei geht es also um die distributive Gerechtigkeit zwischen Gatekeepern und ihren Nutzern.[4]

Verstöße gegen den DMA können mit empfindlichen Geldbußen in Höhe von bis zu 10 % beziehungsweise bei Wiederholungstaten 20 % des im vorausgegangenen Geschäftsjahr weltweit erzielten Gesamtumsatzes geahndet werden, vgl. Art. 30 DMA. Daneben können Dritte die Verpflichtungen aus dem DMA auch im Wege der privaten Rechtsdurchsetzung nach §§ 33 ff. Gesetz gegen Wettbewerbsbeschränkungen (GWB), § 3a Gesetz gegen den unlauteren Wettbewerb (UWG) oder über § 823 Abs. 2 Bürgerliches Gesetzbuch (BGB) geltend machen.[5]

1 Vgl. Lettl, WM 2025, 1161 (1165)

2 Vgl. Podszun/Schwab in: Podszun, DMA Art. 5 Rn. 3.

3 Käseberg/Gappa in: Podszun, DMA Art. 1 Rn. 6; siehe auch Erwägungsgrund Nr. 32 zum DMA.

4 Käseberg/Gappa in: Podszun, DMA Art. 1 Rn. 7; siehe auch Erwägungsgrund Nr. 33 zum DMA.

5 Podszun/Schwab in: Podszun, DMA Art. 5 Rn. 6.

## a. Gatekeeper

Adressaten des DMA sind die sogenannten Gatekeeper (Torwächter), die von der Europäischen Kommission nach Art. 3 DMA anhand ökonomischer Kriterien als solche benannt werden müssen. Derzeit umfasst die Liste der Gatekeeper sechs Unternehmen: Alphabet (Mutterkonzern von Google) Amazon, Apple, Booking.com, ByteDance (Mutterkonzern von TikTok), Microsoft sowie Meta Platforms (Mutterkonzern von Facebook, Instagram und WhatsApp).[6]

Bei der Benennung der Gatekeeper muss die Kommission nicht nur das Unternehmen selbst, sondern auch den jeweiligen Plattformdienst benennen, auf dem das Unternehmen seine „Torwächterstellung" ausübt, vgl. Art. 3 Abs. 9 DMA.[7]

## b. Verhaltenspflichten

Herzstück des DMA bilden die detaillierten Verhaltenspflichten der Gatekeeper nach Art. 5-7 DMA.[8] Diese greifen tief in die unternehmerischen Entscheidungen der Gatekeeper ein und haben das Potenzial, das Erscheinungsbild zahlreicher digitaler Produkte und Dienstleistungen in den nächsten Jahren nachhaltig zu verändern und zu prägen. Im Folgenden soll daher ein kurzer – keinesfalls vollständiger – Überblick über die teils als Gebote, teils als Verbote formulierten Vorschriften gegeben werden.

Art. 5 Abs. 2 DMA sieht etwa ein Verbot der Datenzusammenführung vor. Gatekeeper dürfen danach ohne explizite Zustimmung der Endnutzer personenbezogene Daten nicht mehr zu einem integrierten Datensatz zusammenführen. Hierdurch soll die Machtkonzentration durch umfassende Datenakkumulation aus verschiedenen Datenquellen verhindert werden, was eine Bestreitbarkeit der Märkte verspricht.

In Art. 5 Abs. 3 DMA findet sich ein Verbot von Paritätsklauseln. Das sind vertragliche Bedingungen des Gatekeepers, die gewerbliche Nutzer daran hindern, Endnutzern dieselben Produkte oder Dienstleistungen über Online-Vermittlungsdienste Dritter oder über ihre eigenen direkten Online-Vertriebskanäle zu anderen Preisen oder Bedingungen anzubieten als über die Online-Vermittlungsdienste des Gatekeepers.

Die wichtigsten Verbote dürften die Anti-Steering Maßnahmen nach Art. 5 Abs. 4 DMA sein. Hierbei handelt es sich um Maßnahmen gegen Vertragsbedingungen, durch die Gatekeeper gewerbliche Nutzer daran hindern, ihren zentralen Plattformdienst zur Kundengewinnung zu nutzen, um die Kunden dann anschließend auf eigene Internetseiten der gewerblichen Nutzer oder andere Plattformen umzuleiten.[9] Anti-Steering Regeln waren in der Vergangenheit bereits häufiger Gegenstand der Kartellrechtspraxis, als in mehreren Ländern Wettbewerbsbehörden gegen das App-Store-Design von Apple vorgegangen sind.[10] Ziel von Art 5 Abs. 4 DMA ist daher, gewerblichen Nutzern zu erlauben, die Kommunikation mit den Endnutzern auch außerhalb des zentralen Plattformdienstes des Gatekeepers zu führen. Die Interaktionen auf der Plattform müssen dabei so ausgestaltet werden, dass der gewerbliche Nutzer sich frei für einen Vertriebskanal entscheiden kann.

Nach Art. 5 Abs. 5 DMA muss Endnutzern der Zugriff auf Dienste oder digitale Inhalte ermöglicht werden, die sie außerhalb der Plattform des Gatekeepers erworben haben. Hierdurch sollen sogenannte Lock-in-Effekte verhindert und die Nutzung interoperabler Dienste gefördert werden.[11]

Art. 6 Abs. 2 DMA statuiert ein Verbot der Datenverwendung. Gatekeeper dürfen nicht öffentlich zugängliche Daten, die von gewerblichen Nutzern generiert oder bereitgestellt werden, nicht für eigene Zwecke nutzen, soweit diese Nutzung im Wettbewerb mit den gewerblichen Nutzern stehen kann. So soll verhindert werden, dass der Gatekeeper in einer Doppelrolle als

6 https://digital-markets-act.ec.europa.eu/gatekeepers_en.

7 Käseberg/Gappa in: Podszun, DMA Art. 3 Rn. 28.

8 Podszun/Schwab in: Podszun, DMA Art. 5 Rn. 1.

9 Heinz in: Podszun, DMA Art. 5 Rn. 62.

10 Vgl. hierzu Heinz in: Podszun, DMA Art. 5 Rn. 65.

11 Vgl. hierzu Heinz in: Podszun, DMA Art. 5 Rn. 92f.

Plattformbetreiber und Wettbewerber auftreten kann.[12]
Art. 6 Abs. 3 DMA regelt den Umgang mit herstellerseitig vorinstallierter Software und Default-Einstellungen. Gatekeeper müssen hiernach Endnutzern die Möglichkeit geben, vorinstallierte Software-Anwendungen zu deinstallieren und Standardeinstellungen bei Betriebssystemen, virtuellen Assistenten und Webbrowsern zu ändern.[13] Hierfür müssen sie die Endnutzer aktiv auffordern, eine Entscheidung zu treffen, vgl. Art. 6 Abs. 3 UAbs. 2 S. 2 DMA.

Nach Art. 6 Abs. 4 DMA müssen Gatekeeper es Endnutzern ermöglichen, Drittanbieter-Software und -App-Stores auf ihren Plattformen zu installieren, was auch den Download von Apps und App-Stores außerhalb des App-Stores des Gatekeepers (Sideloading) erfasst.[14] Es bleibt ihnen dabei allerdings möglich, unbedingt erforderliche und angemessene Maßnahmen zur Wahrung der Systemintegrität zu treffen.

## II. Die ersten Bußgeldverfahren

Nach längerer vorangegangener Untersuchung hat die Europäische Kommission am 22. April 2025 gegen die Unternehmen Apple und Meta nun erstmalig Verstöße gegen den DMA festgestellt und Bußgelder in Höhe von 500 Millionen Euro (Apple) und 200 Millionen Euro (Meta) verhängt.[15]

### a. Apple Appstores

Apple wurde als Anbieter im Bereich mobiler Betriebssysteme und App-Vertriebsplattformen von der Europäischen Kommission als Gatekeeper eingestuft. Apple kontrolliert seinen eigenen App-Store streng hinsichtlich der Art und Weise, wie Entwickler ihre Apps vertreiben und wie Endnutzer auf diese Apps zugreifen können. Die Kommission monierte insbesondere die Beschränkung der App-Entwickler, ihre Kunden frei zu lenken („steering"), sowie die Einschränkung von sogenannten Link-Outs, mit denen gewerbliche Nutzer ihre Endkunden auf andere Webseiten außerhalb des Apple-Ökosystems locken können.
Im August 2024 hatte Apple der Europäischen Kommission zwar Änderungen vorgeschlagen, die ein Steering durch gewerbliche Nutzer ermöglichen sollte. Diese waren jedoch mit erheblichen Gebühren verbunden. So sollten gewerbliche Nutzer eine „initial acquisition fee" von 5 % für die Akquisition eines Endnutzers über den Apple App Store zahlen, welche sich auf alle Verkäufe digitaler Güter und Dienstleistungen innerhalb von 12 Monaten nach der Installation berechnet. Daneben forderte Apple eine zusätzliche 10 %ige „store services fee" auf Käufe, die über Link-Outs getätigt werden.[16]

Außerdem verpflichtete Apple die Entwickler dazu, beim Weiterleiten von Nutzern einen In-App-Hinweisbildschirm anzuzeigen. Diese sogenannten „Scare Screens" warnen Nutzer davor, dass ihre Privatsphäre und Sicherheit nun vom Entwickler und somit nicht mehr direkt von Apple verwaltet werden. Hierdurch wurden Verbraucher abgeschreckt und das Steering durch die App-Entwickler behindert.

Gemäß Art. 5 Abs. 4 DMA ist Apple als Gatekeeper verpflichtet, es seinen gewerblichen Nutzern, also den App-Entwicklern, zu ermöglichen, Endnutzer kostenlos über alternative Angebote außerhalb des hauseigenen App-Stores zu informieren. Zudem müssen App-Entwickler in der Lage sein, Endnutzer auf solche Angebote aufmerksam zu machen und auch außerhalb des App-Stores mit ihnen Verträge abzuschließen.

Am 23. April 2025 verhängte die Kommission schließlich ein Bußgeld über eine halbe Milliarde Euro gegen Apple und ordnete konkret an, die technischen und kommerziellen Beschränkungen des Steerings zu beseitigen und künftig von gleichartigen Verstößen abzusehen. Anderenfalls drohen Zwangsgelder.

12 Wolf-Posch in: Podszun, DMA Art. 6 Rn. 4.

13 Herbers in: Podszun, DMA Art. 6 Rn. 23.

14 Herbers in: Podszun, DMA Art. 6 Rn. 53.

15 https://germany.representation.ec.europa.eu/news/verstosse-gegen-das-gesetz-uber-digitale-markte-dma-millionen-geldbussen-fur-apple-und-meta-2025-04-23_de.

16 Siehe hierzu https://developer.apple.com/support/communication-and-promotion-of-offers-on-the-app-store-in-the-eu/.

### b. Meta Pay or Consent

Das sogenannte „Pay or Consent"-Modell – auch als „Consent or Pay", „Pay or Okay" oder „Pur Abo" bezeichnet – stellt Nutzer vor eine Wahlentscheidung beim Zugang zu Online-Diensten.[17] Nach der Definition des Europäischen Datenschutzausschusses (EDSA) handelt es sich um Modelle, bei denen Anbieter betroffenen Personen mindestens zwei alternative Zugangswege zu ihren Online-Diensten anbieten.

Der Hintergrund der Einführung des „Consent or Pay"-Modells von Meta ist datenschutzrechtlicher Natur: Die irische Datenschutzbehörde Data Protection Commission (DPC) hatte entschieden, dass Meta sich für ihr kommerzielles Geschäftsmodell, die Verarbeitung personenbezogener Daten zur Schaltung personalisierter Werbung, nicht auf die datenschutzrechtlichen Rechtsgrundlagen des berechtigten Interesses (Art. 6 Abs. 1 lit. f Datenschutz-Grundverordnung (DSGVO)) oder die Notwendigkeit zur Vertragserfüllung (Art. 6 Abs.1 lit. b DSGVO) stützen könne. Meta blieb somit nur die Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO als Rechtsgrundlage. Damit diese als „freiwillig erteilt" gelten kann, muss dem Betroffenen jedoch eine Alternative geboten werden. Diese sollte in der Zahlung eines Betrags von 9,99 Euro im Monat bestehen, bei der keine Verarbeitung personenbezogener Daten zu Werbezwecken erfolgt.

Meta führte auf seinen Plattformen Facebook und Instagram also ein binäres Consent or Pay-Modell ein, wonach Nutzer entweder in die Verarbeitung ihrer personenbezogenen Daten einwilligen oder ein kostenpflichtiges monatliches Abonnement abschließen müssen.

Die Kommission sah hierin einen Verstoß gegen Art. 5 Abs. 2 DMA, da ein solches Modell nicht feingranular genug sei, um dem Nutzer tatsächlich eine gleichwertige, weniger privatsphäreinvasive Nutzungsmöglichkeit zu bieten. Zudem sah das binäre Consent or Pay-Modell keine „spezifische Wahl" vor, um in die nach Art. 5 Abs. 2 lit. a –c DMA genannten Nutzungszwecke einzuwilligen, insbesondere nicht in die Zusammenführung personenbezogener Daten aus mehreren Plattformdiensten, in diesem Fall zum Beispiel Facebook und Instagram.

In der Zwischenzeit führte Meta im November 2024 eine überarbeitete Version ein, die tatsächlich eine kostenlose Option für „weniger personalisierte Werbung" bietet. Die Kommission prüft derzeit noch, ob diese auch den Anforderungen des DMA entspricht.[18] Die Verhängung der Strafe in Höhe von 200 Mio. Euro erfolgte dagegen bereits wegen des Verstoßes gegen das Verbot der Datenzusammenführung aus Art. 5 Abs. 2 DMA für den Zeitraum zwischen Anwendbarkeit des DMA (März 2024) und der Einführung der überarbeiteten Consent or Pay Option (November 2024).

## III. Ausblick

Der DMA hat sich von einem theoretischen Regulierungsrahmen zu einem scharfen Schwert der digitalen Marktregulierung entwickelt. Die ersten Bußgelder sind dabei nur der Anfang einer längeren Entwicklung, die die digitale Wirtschaft nachhaltig prägen wird. Für die Gatekeeper bedeutet dies eine fundamentale Neuausrichtung ihrer Geschäftspraktiken – für Verbraucher und gewerbliche Nutzer hingegen die Aussicht auf mehr Wahlfreiheit und fairere Marktbedingungen. Die ersten Reaktionen der Gatekeeper auf die Einschätzungen der Europäischen Kommission lassen den Schluss zu, dass die Unternehmen das neue Instrumentarium der Digitalregulierung durchaus ernst nehmen. Die kommenden Monate werden zeigen, ob der DMA sein ambitioniertes Versprechen einlösen kann, die digitalen Märkte nachhaltig zu öffnen und zu demokratisieren. Weitere Verfahren laufen derzeit gegen Alphabet (Google Play und Google Search) sowie gegen Apple wegen weiterer DMA-Verstöße. Eine rechtliche Überprüfung der verhängten Strafen wurde durch Apple und Meta angekündigt.

17 Kollmann, DSB 2025, 158 (158).

18 https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085.

# Cybersicherheit an Hochschulen in Europa – eine Übersicht

## Das europäische Cybersicherheitsrecht hat sich in den letzten Jahren rasant weiterentwickelt – Zeit für einen hochschulspezifischen Überblick

*Von Philipp Schöbel, Berlin*

Die voranschreitende Digitalisierung des Hochschulsektors birgt enorme Chancen, aber auch Risiken. Auch deutsche Hochschulen waren in der Vergangenheit von Cyberattacken betroffen. Die Folgen können dabei Forschung, Lehre und Verwaltung gleichermaßen treffen. Die Europäische Union hat in den vergangenen Jahren viele neue Sekundärrechtsakte mit Digitalbezug erlassen. Auch im Bereich des Cybersicherheitsrechts sind neue Rechtsakte und regulatorische Instrumente hinzugekommen. Bevor in zukünftigen Ausgaben des Infobriefs Recht vertieft auf die Einzelheiten bestimmter Rechtsakte eingegangen wird, soll hier zunächst ein grundlegender Überblick geschaffen werden.

## I. Welche europäischen Rechtsakte gibt es?

Auf europäischer Ebene existieren verschiedene Sekundärrechtsakte, die das Themenfeld Cybersicherheit regeln. Dazu gehören der Cybersecurity Act (CSA),[1] die Verordnung über Cybersolidarität (CyberSoli-VO),[2] die NIS-2-Richtlinie (NIS-2-RL),[3] der Cyber Resilience Act (CRA)[4] oder auch sektorspezifische Rechtsakte wie die Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA)[5]. Daneben beinhalten Digitalrechtsakte,

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

2 Verordnung (EU) 2025/38 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung von, Vorsorge für und Bewältigung von Cyberbedrohungen und Sicherheitsvorfällen und zur Änderung der Verordnung (EU) 2021/694 (Cybersolidaritätsverordnung), ABl. L 2025/38 S. 1.

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

4 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), Ablauf. L. 2024/2847, S. 1.

5 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, ABl. L. 333 S. 1.

wie die Datenschutz-Grundverordnung (DSGVO)[6] oder die Verordnung über Künstliche Intelligenz (KI-VO)[7] auch einzelne Vorschriften zur Cybersicherheit. Nicht alle diese Rechtsakte sind gleichsam für den Hochschulsektor relevant. Daher werden im Folgenden der jeweilige Zweck und die Instrumente der genannten Rechtsakte kurz dargestellt, um einen Überblick zu schaffen. Allein die Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA) soll an dieser Stelle wegen ihres offensichtlich fehlenden Hochschulbezugs ausgespart werden. Die Regelungen zur Cybersicherheit in der KI-VO[8] und der DSGVO werden aus Platzgründen auch in einem kommenden Beitrag im Infobrief dargestellt.

## II. Der Cybersecurity Act

Der CSA stärkt zum einen die Agentur der Europäischen Union für Cybersicherheit (ENISA).[9] Dies geschieht, indem diese ein ständiges Mandat, neue Aufgaben und mehr Ressourcen erhält. Zum anderen wird mit dem CSA ein Rahmen für die Cybersicherheitszertifizierung von Produkten und Dienstleistungen geschaffen. Dieser neue europäische Rahmen für die Cybersicherheitszertifizierung gilt für Produkte, Dienste und Prozesse der Informations- und Kommunikationstechnologie (IKT). Die Europäische Agentur für Cybersicherheit übernimmt eine zentrale Funktion beim Aufbau und der Pflege des gesamteuropäischen Zertifizierungsrahmens für Cybersicherheit, wobei sie die technische Basis für einzelne Zertifizierungsverfahren entwickelt. Zu ihren Aufgaben gehört es, die Bevölkerung mittels einer eigenen Online-Plattform über verfügbare Zertifizierungsverfahren und erteilte Zertifikate zu unterrichten. ENISA hat zudem den Auftrag erhalten, die operative Kooperation zwischen den EU-Staaten zu intensivieren und denjenigen Mitgliedstaaten, die entsprechende Hilfe anfordern, bei der Bewältigung von Cybersicherheitsereignissen beizustehen. Darüber hinaus soll die Agentur die europäische Koordination unterstützen, wenn es zu umfangreichen länderübergreifenden Cyberattacken oder entsprechenden Krisensituationen kommt.

## III. Die Verordnung über Cybersolidarität

Die CyberSoli-VO enthält Maßnahmen zur Stärkung der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cyberbedrohungen und Sicherheitsvorfällen (vgl. Art. 1 Abs. 1 CyberSoli-VO). Dafür wird ein „europäisches Warnsystem für Cybersicherheit“ eingerichtet, um Fähigkeiten zur koordinierten Erkennung und gemeinsamen Lageerfassung aufzubauen und zu verbessern (Art. 1 Abs. 1 lit a) CyberSoli-VO). Weiterhin wird ein sogenannter Cybernotfallmechanismus begründet. Dieser soll die Mitgliedstaaten und andere Nutzer bei der Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes unterstützen (Art. 1 As. 1 lit b) CyberSoli-VO). Der Cybernotfallmechanismus besteht aus Unterstützung von Vorsorgemaßnahmen, der Einrichtung einer EU-Cybersicherheitsreserve und Gewährleistung der gegenseitigen Amtshilfe.[10] Die EU-Cybersicherheitsreserve wird aus Reaktionsdiensten privater Diensteanbieter bestehen, die auf Ersuchen der Mitgliedstaaten oder der EU eingesetzt werden können, um diese bei der Bewältigung schwerwiegender Cybersicherheitsvorfälle zu unterstützen. Schließlich wird auch ein europäischer Überprüfungsmechanismus für Cybersicherheitsvorfälle etabliert. Dieser dient dazu, schwerwiegende Cybersicherheitsvorfälle zu überprüfen und zu bewerten (Art. 1 As.1 lit c) CyberSoli-VO). Die Verordnung über Cybersolidarität enthält keine hochschulspezifischen Cybersicherheitspflichten.

---

6 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 (Datenschutz-Grundverordnung), ABl. L. 119 S. 1.

7 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.

8 Siehe zur KI-VO: Schöbel, AI Act – Licht der Europäischen Union?, DFN-Infobrief Recht 12 / 2024, S. 7; derselbe, Der AI Act und die Wissenschaft, DFN-Infobrief Recht 2 / 2025, S. 2; derselbe, KI-Modelle made in Europe?, DFN-Infobrief Recht 4 / 2025, S. 14.

9 Siehe zu diesem Absatz insgesamt: Europäische Kommission, Der EU-Rechtsakt zur Cybersicherheit, abrufbar unter: https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-act, (alle Onlinequellen zuletzt abgerufen am 28. Juli 2025).

10 Europäische Kommission, Der EU-Rechtsakt zur Cybersolidarität, abrufbar unter: https://digital-strategy.ec.europa.eu/de/policies/cybersolidarity.

## IV. Die NIS-2-Richtlinie

Die NIS-2-RL ersetzt die frühere NIS-1-Richtlinie aus dem Jahr 2016.[11] Sie soll einen einheitlichen Rechtsrahmen für die Aufrechterhaltung der Cybersicherheit in 18 kritischen Sektoren in der gesamten EU schaffen.[12] Die Mitgliedstaaten sollen zudem nationale Cybersicherheitsstrategien festlegen. Diese umfassen die Strategien für die Sicherheit der Lieferketten, das Schwachstellenmanagement sowie die Aufklärung und Sensibilisierung im Bereich der Cybersicherheit. Zudem sollen sie bei grenzüberschreitenden Reaktionen im Falle von Cybersicherheitsvorfällen und der Durchsetzung mit der EU zusammenarbeiten. Die Regelungen der NIS-2-RL sollen die europäischen Cybersicherheitsstandards erheblich verbessern, indem sie den Geltungsbereich erweitern, präzisere Regelungen etablieren und wirksamere Überwachungsmechanismen implementieren. Die EU-Mitgliedstaaten sind nun dazu angehalten, ihre digitalen Abwehrkapazitäten auszubauen. Gleichzeitig müssen Organisationen aus einer größeren Anzahl von Wirtschaftssektoren Risikomanagement-Protokolle umsetzen und Sicherheitsvorfälle melden. Die Richtlinie etabliert außerdem Rahmenwerke für die grenzüberschreitende Kooperation, den Austausch sicherheitsrelevanter Informationen sowie die Überwachung und Umsetzung von Cyberschutzmaßnahmen. Durch Aufsichtsmechanismen, Durchsetzungsverfahren und freiwillige Evaluierungen zwischen den Mitgliedstaaten sollen das Vertrauen gestärkt und die Cybersicherheitskompetenz unionsweit verbessert werden. Ein wichtiger Aspekt ist dabei die direkte Verantwortlichkeit der Unternehmensführung für Versäumnisse beim Cybersicherheitsrisikomanagement, wodurch Cybersicherheit „zur Chefsache“ wird. „Die Mitgliedstaaten müssen außerdem eine Liste der Betreiber wesentlicher Dienste erstellen und regelmäßig aktualisieren, um sicherzustellen, dass diese Einrichtungen die Anforderungen der Richtlinie erfüllen.“ Mit der Richtlinie wird ein Netzwerk von Computer Security Incident Response Teams (CSIRTs) eingerichtet.[13] Dieses dient dazu, Informationen über Cyberbedrohungen auszutauschen und auf Vorfälle zu reagieren. Außerdem wird damit das europäische Netz der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe)[14] geschaffen, um Cybersicherheitsvorfälle oder -krisen großen Ausmaßes zu bewältigen.

Ergänzend wurde mit der NIS-Kooperationsgruppe[15] eine Plattform geschaffen, die als Koordinationsstelle für die strategische Vernetzung und den Austausch relevanter Informationen zwischen den europäischen Mitgliedstaaten, der Kommission und der Europäischen Agentur für Cybersicherheit (ENISA) fungiert. Diese Arbeitsgruppe erstellt nicht bindende Richtlinien und Handlungsempfehlungen, die den Mitgliedstaaten bei der praktischen Implementierung der NIS-Bestimmungen als Orientierungshilfe dienen.[16]

Anhang I der NIS-2-RL legt elf verschiedene sogenannte „Sektoren hoher Kritikalität“ fest. Hier werden unter dem Sektor „8. Digitale Infrastruktur“ verschiedene Arten von Einrichtungen genannt. Diese umfassen unter anderem Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten und Vertrauensdiensteanbieter. Diese Begriffe werden in Art. 6 der NIS-2-RL legaldefiniert. In Anhang II werden sieben „Sonstige kritische Sektoren“ festgelegt – einer davon ist die Forschung. In Deutschland fehlt es bislang weiterhin an einem nationalen Umsetzungsgesetz. Nachdem im Infobrief bereits über den Entwurf eines Umsetzungsgesetzes der alten Bundesregierung[17] berichtet wurde[18], hat das Bundesministerium des Innern

11 Siehe zur Reform der NIS1-Richtlinie: John, CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS?, DFN-Infobrief Recht 4 / 2023, S. 6.

12 Siehe zu diesem Absatz insgesamt die Darstellung der Europäischen Kommission, NIS2-Richtlinie: Sicherung von Netz- und Informationssystemen, letzte Aktualisierung 1.Juli 2025, abrufbar unter: https://digital-strategy.ec.europa.eu/de/policies/nis2-directive.

13 ENISA, ENISA serves as the CSIRTs Network's secretariat and supports the cooperation and coordination of CSIRTs during cybersecurity incidents, abruafbar unter: https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/csirts-network.

14 Siehe dazu auch ENISA, ENISA serves as the CyCLONe Secretariat boosting cooperation among national Cyber Crises Liaison Organisations, abrufbar unter: https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone.

15 Weitere Informationen zur NIS-Kooperationsgruppe: Europäische Kommission, NIS-Kooperationsgruppe, abrufbar unter: https://digital-strategy.ec.europa.eu/de/policies/nis-cooperation-group.

16 Europäischen Kommission, NIS2-Richtlinie: Sicherung von Netz- und Informationssystemen, letzte Aktualisierung 1.Juli 2025, abrufbar unter: https://digital-strategy.ec.europa.eu/de/policies/nis2-directive.

17 BT-Drs. 20/13184 vom 02.10.2024, weiterhin abrufbar unter https://dserver.bundestag.de/btd/20/131/2013184.pdf.

18 Geiselmann, Heute schon geNISt?, DFN-Infobrief Recht 4 / 2025 | Seite 9.

mittlerweile einen neuen Referentenentwurf[19] vorgelegt. Über die Umsetzung der NIS-2-Richtlinie wird in einer kommenden Ausgabe des Infobriefs Recht ausführlich berichtet. Inwieweit die NIS-2-Richtlinie auch Hochschulen hinsichtlich ihrer Cybersicherheit verpflichtet, kann erst nach der Verabschiedung des deutschen Umsetzungsgesetzes vollständig geklärt werden.

## V. Der Cyber Resilience Act

Der CRA[20] gehört zum europäischen Produktsicherheitsrecht nach dem sogenannten „Neuen Rechtsrahmen" (NLF).[21] [22] Der CRA bedarf als Verordnung keines deutschen Umsetzungsgesetzes und wird ab dem 11. Dezember 2027 gelten (Art. 71 Abs. 2 CRA).[23] Der CRA soll die Cybersicherheitsstandards von Produkten, die eine digitale Komponente enthalten, verbessern.[24] Hersteller und Einzelhändler werden verpflichtet, die Cybersicherheit dieser Produkte während des gesamten Lebenszyklus ihrer Produkte sicherzustellen. Die neue Verordnung etabliert rechtlich bindende Sicherheitsstandards für Hersteller und Händler. Diese betreffen sämtliche Phasen von der Konzeption über die Gestaltung und Herstellung bis hin zur Instandhaltung entsprechender Produkte. Anforderungen an Produkte, die eine digitale Komponente enthalten, sind entlang der gesamten Lieferkette zu befolgen. Zusätzlich sind die Hersteller dazu angehalten, über die komplette Nutzungsdauer ihrer Erzeugnisse hinweg Betreuungsleistungen zu erbringen. Besonders sicherheitskritische Produkte müssen vor ihrer Markteinführung in der EU außerdem einer unabhängigen Prüfung durch akkreditierte Bewertungsstellen unterzogen werden. Die neuen Regelungen erfassen sämtliche Produkte, die eine direkte oder indirekte Verbindung zu anderen Geräten oder Netzwerken aufweisen. Ausgenommen sind jedoch bestimmte Bereiche wie spezielle Open-Source-Software oder Dienstleistungen sowie Produkte, die bereits anderen Regelwerken unterliegen – beispielsweise aus der Medizintechnik, Luftfahrt oder Automobilbranche. Konforme Produkte erhalten die bekannte CE-Kennzeichnung[25] als Nachweis für die Erfüllung der gesetzlichen Anforderungen. Die neue Rechtslage verschiebt die Verantwortung stärker zu den Herstellern, die gewährleisten müssen, dass ihre digitalen Produkte den europäischen Cybersicherheitsvorgaben genügen. Dadurch sollen Verbraucher die Möglichkeit erhalten, eine informierter Kaufentscheidung zu treffen und auf die Cybersicherheit CE-gekennzeichneter Produkte zu vertrauen.

## VI. Ausblick

Der Rechtsrahmen des europäischen Cybersicherheitsrechts ist komplex, aber nicht unüberschaubar. Wie oben bereits angekündigt, sollen die einschlägigen Rechtsakte in den kommenden Ausgaben detaillierter dargestellt werden. Besonders interessant wird aller Voraussicht nach die Umsetzung der NIS-2-RL sein. Hochschulen sollten sich bestenfalls vor dem Eintreten konkreter Cybersicherheitsvorfälle mit den neuen europäischen Rechtsakten beschäftigen. Hochschulen, die selbst keine Produkte im Sinne des CRA herstellen, dürften vor allem von der NIS-2-RL betroffen sein. Die Verordnung über europäische Cybersolidarität dürfte aus Compliance-Sicht für Hochschulen wenig relevant sein. Der CSA ist vor allem dann von praktischer Bedeutung, wenn die Cybersicherheitszertifizierung von Produkten und Dienstleistungen an Hochschulen bewertet werden soll.

---

19 BMI, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, 23.06.2025, abrufbar unter: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-RefE_2025.pdf?__blob=publicationFile&v=9.

20 Zum Entwurf des CRA siehe: Palenberg, Cyber Angriff ade mit dem CRA-E?, DFN-Infobrief Recht 9 / 2023, S. 2; Tech, Die Bretonage der europäischen Datenstrategie, DFN-Infobrief Recht 4 / 2024, S. 8.

21 Die gängige Abkürzung NLF steht für „New legislative framework".

22 Europäische Kommission, Neuer Rechtsrahmen, abrufbar unter: https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en?prefLang=de&etrans=de.

23 Einzelne Vorschriften gelten Juni respektive September 2026 (Art. 71 Abs. 2 UAbs. 2 CRA).

24 Europäische Kommission, Cyberresilienzgesetz (Cyber Resilience Act), abrufbar unter: https://digital-strategy.ec.europa.eu/de/policies/cyber-resilience-act.

25 Weitere Informationen zur CE-Kennzeichnung finden sich unter: Your Europe, CE-Kennzeichnung, abrufbar unter: https://europa.eu/your-europe/business/product-requirements/labels-markings/ce-marking/index_de.htm.

# DFN Infobrief-Recht-Aktuell

- ## Datenschutzrecht: Verwaltungsgericht (VG) Köln zur Klage des Bundes gegen die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) zum Betrieb der Facebook-Fanpage des Bundespresseamtes

  Die BfDI untersagte dem Bundespresseamt den Betrieb einer Fanpage wegen Verstößen gegen die Datenschutz-Grundverordnung (DSGVO). Durch die nicht datenschutzkonforme Ausgestaltung des von Meta genutzten Cookie-Banners liege keine wirksame Einwilligung für die Speicherung und das Auslesen bestimmter Cookies vor. Zudem handele es sich um eine gemeinsame Verantwortlichkeit mit Meta. Hiergegen wandten sich sowohl die Bundesregierung als auch Meta. Das VG Köln war nun in seiner Entscheidung der Auffassung, dass nicht das Bundespresseamt, sondern Meta zur Einholung einer Einwilligung verpflichtet sei und lehnte eine gemeinsame Verantwortlichkeit ab.

  Hier erhalten Sie den Link zur Pressemitteilung:
  https://www.vg-koeln.nrw.de/behoerde/presse/Pressemitteilungen/08_22072025/index.php

- ## Strafrecht/Medienrecht: Urteil des Amtsgerichts Tiergarten vom 23. Juli 2025 zu den Posts des Comedian und Satirikers Sebastian Hotz

  Der Satiriker und Comedian Sebastian Hotz hatte nach dem Attentat auf Donald Trump im Juli 2024 eine Nachricht auf der Plattform X verbreitet, die dazu veranlasste, gegen ihn wegen der Billigung von Straftaten nach § 140 Nr. 2 Strafgesetzbuch Anklage zu erheben. Das Amtsgericht Tiergarten sprach ihn nun frei. Es vertritt die Auffassung, dass es sich um Satire handele, die ersichtlich nicht geeignet sei, den öffentlichen Frieden zu stören.

  Hier erhalten Sie den Link zur Pressemitteilung:
  https://www.berlin.de/gerichte/presse/pressemitteilungen-der-ordentlichen-gerichtsbarkeit/2025/pressemitteilung.1583436.php

- ## Medienrecht: Referentenentwurf zur Anti-SLAPP-Richtlinie des Bundesministeriums für Justiz und Verbraucherschutz (BMJV)

  Die Europäische Union hat 2024 eine Richtlinie verabschiedet, um Einschränkungsklagen gegen Journalisten entgegenzuwirken. SLAPP (Strategic Lawsuits Public Participation) sind missbräuchliche Klagen, die sich vor allem gegen Journalist:innen, Aktivist:innen und NGOs richten. Sie haben die Absicht, kritische Stimmen aus der öffentlichen Debatte zu verdrängen. Hiergegen richtet sich die Anti-SLAPP-Richtlinie. Sie ist bis zum 7. Mai 2026 in nationales Recht umzusetzen. Das BMJV hat nun einen Referentenentwurf vorgestellt.

  Hier erhalten Sie den Link zum Referentenentwurf:
  https://www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_Anti_SLAPP.pdf?__blob=publicationFile&v=4

# Kurzbeitrag: Gut gemeint, doch schlecht gemacht: Bundesverfassungsgericht kippt Postdoc-Paragraf für Berliner Hochschulen

## Das Land Berlin scheitert mit dem Versuch, Hochschulen zu verpflichten, Postdocs Dauerstellen anzubieten

*von Pascal Sonak, Münster*

Gemäß einer Regelung des Berliner Hochschulgesetzes (BerlHG) mussten promovierte Nachwuchswissenschaftler:innen, mit dem Ende ihres Arbeitsvertrages, eine Anschlusszusage für eine unbefristete Beschäftigung erhalten. Die Humboldt-Universität zu Berlin (HU) erhob dagegen im Jahr 2021 Verfassungsbeschwerde vor dem Bundesverfassungsgericht (BVerfG). Mit Erfolg: Die Richterinnen und Richter des Ersten Senats erklärten die Regelung für nicht vereinbar mit den Vorschriften des Grundgesetzes (BVerfG Urt. v. 25.06.2025 - 1 BvR 368/22).

## I. Hintergrund

Die HU erhob im Jahr 2021 Verfassungsbeschwerde gegen eine Vorschrift des zu diesem Zeitpunkt neu erlassenen BerlHG. Konkret richtete sich die Verfassungsbeschwerde der HU gegen den § 110 Abs. 6 S. 2 BerlHG. Dieser sah eine Pflicht für Hochschulen vor, allen befristet eingestellten wissenschaftlichen Mitarbeiter:innen mit einer Promotion den Abschluss eines unbefristeten Beschäftigungsverhältnisses für den Fall der erfolgreichen Qualifizierung zuzusichern. Dem hielt die HU entgegen, dass dem Land Berlin bereits die erforderliche Gesetzgebungskompetenz fehle. Zudem sei der mit dem § 110 Abs. 6 S. 2 BerlHG einhergehende Eingriff in die grundgesetzlich geschützte Wissenschaftsfreiheit der Universität aus Art. 5 Abs. 3 S. 1 Grundgesetz (GG) nicht verhältnismäßig.

Exkurs: Grundrechtsberechtigung

Grundsätzlich handelt es sich bei den Grundrechten der Art. 1 bis 19 GG um „Abwehrrechte des Bürgers gegen den Staat“[1] . Sie führen zu einer Verpflichtung des Staates, ungerechtfertigte Eingriffe in grundrechtliche Schutzgüter zu unterlassen; der Staat ist grundrechtsverpflichtet. Die Abwehrfunktion der Grundrechte wird dabei insbesondere durch die Möglichkeit ihrer Einklagbarkeit zum Ausdruck gebracht.[2] Im Rahmen der sog. „Ausnahmetrias“[3] sind allerdings auch staatliche Universitäten, die in der Form der Körperschaft des öffentlichen Rechts organisiert sind (vgl. zum Beispiel § 2 Abs. 1 S. 1 Hochschulgesetz NRW), der Wissenschaftsfreiheit gemäß Art. 5 Abs. 3 GG unmittelbar zugeordnet und somit (nur) dahingehend grundrechtsberechtigt. Anderenfalls wäre die institutionelle Funktionsfähigkeit der Einrichtungen hinsichtlich Wissenschaft, Forschung und Lehre nicht ausreichend gewährleistet.[4]

1 BVerfG Urt. v. 15.01.1958 - 1 BvR 400/51 Rn. 24.

2 Sauer, Dreier Grundgesetz-Kommentar 4. Auflage 2023, Art. 1 GG Rn. 96.

3 Kaufhold, Dreier Grundgesetz-Kommentar 4. Auflage 2023, Art. 3 GG Rn. 60 f.

4 Vgl. BVerfG Urt. v. 29.05.1973 - 1 BvR 424/71, 1, 1 BvR 325/72.

## II. Entscheidung

Mit ihrem Beschluss vom 25.06.2025 entsprachen die Richter:innen des BVerfG nun weitgehend den Forderungen der Klägerin.

Die in § 110 Abs. 6 S. 2 BerlHG geregelte Pflicht zur Erteilung einer auf eine Dauerbeschäftigung gerichteten Anschlusszusage greift in die Wissenschaftsfreiheit der HU Berlin gemäß Art. 5 Abs. 3 GG ein.

Diese schützt sowohl die freie wissenschaftliche Betätigung als auch die Freiheit der Forschung sowie die Freiheit der forschungsbasierten Lehre gegen staatliche Eingriffe.[5] Umfasst sind dabei auch alle „wissenschaftsrelevanten“[6] Angelegenheiten, die Forschung und Lehre unmittelbar berühren. Hierunter zählen unter anderem Personalentscheidungen in Angelegenheiten der Hochschullehrer:innen und ihrer wissenschaftlichen Mitarbeiter:innen im Rahmen des Prozesses der Gewinnung und der Vermittlung wissenschaftlicher Erkenntnisse sowie die Aufgabe der Hochschule, den akademischen Nachwuchs zu fördern.[7] Negativ gesehen verbietet es Art. 5 Abs. 3 GG, den Wissenschaftsbetrieb in einer Weise zu gestalten, dass die Gefahr einer Funktionsunfähigkeit oder einer Beeinträchtigung des für die wissenschaftliche Betätigung erforderlichen Freiheitsraums herbeigeführt wird.[8]

Die Verpflichtung zur Abgabe von Anschlusszusagen entzieht den Universitäten die Möglichkeit, eigenverantwortliche Entscheidungen darüber zu treffen, ob und welche promovierten wissenschaftlichen Mitarbeiter:innen sie nach erfolgreichem Abschluss der Qualifikation weiter beschäftigen möchten. Vielmehr sind die Universitäten dazu gezwungen, alle wissenschaftlichen Mitarbeiter:innen, die dies wünschen, dauerhaft zu übernehmen. Dies verkürzt unmittelbar die Freiheit der Hochschule zur Auswahl wissenschaftlichen Personals, was sich wiederum negativ auf die Förderung des akademischen Nachwuchses auswirkt.[9]

Es besteht aufgrund dessen ein grundsätzliches Erfordernis, Beschäftigungsverhältnisse des wissenschaftlichen Personals auf Qualifikationsstellen zeitlich befristen zu können.[10]

Der durch die Pflicht zur Erteilung einer auf eine Dauerbeschäftigung gerichteten Anschlusszusage erfolgende Eingriff in die Wissenschaftsfreiheit (Art. 5 Abs. 3 GG) der HU kann allerdings nicht gerechtfertigt werden. Das einschränkende Gesetz („Schranke“) des § 110 Abs. 6 S. 2 BerlHG ist bereits formell verfassungswidrig, da das Land Berlin nicht über die erforderliche Gesetzgebungskompetenz gemäß Art. 74 Abs. 1 Nr. 12 i.V.m. Art. 72 Abs. 1 GG verfügt. Zwar haben nach Art. 70 Abs. 1 GG grundsätzlich die Länder das Recht zur Gesetzgebung, soweit das Grundgesetz nicht dem Bund das Recht der ausschließlichen oder konkurrierenden Gesetzgebung zuweist. Hier ist die Vorschrift des § 110 Abs. 6 S. 2 BerlHG allerdings dem Kompetenztitel des „Arbeitsrechts“ gem. Art. 74 Abs. 1 Nr. 12 GG zuzuordnen, sodass eine konkurrierende Gesetzgebung besteht. Gem. Art. 72 Abs. 1 GG kann das Land Berlin sich also nicht auf eine Gesetzgebungsbefugnis berufen, solange und soweit der Bundesgesetzgeber bereits seinerseits von der Gesetzgebungskompetenz für das Arbeitsrecht Gebrauch gemacht hat. Im vorliegenden Fall hat der Bundesgesetzgeber mit dem Wissenschaftszeitvertragsgesetz (WissZeitVG) eine abschließende Bestimmung zur Dauer und Beendigung von Arbeitsverhältnissen der zur Qualifizierung eingestellten wissenschaftlichen Mitarbeiterinnen und Mitarbeiter mit einer Promotion formuliert, sodass die Sperrwirkung des Art. 72 Abs. 1 GG vorliegend der landesgesetzlichen Regelung des § 110 Abs. 6 S. 2 BerlHG entgegensteht.[11]

## III. Fazit

Die Möglichkeit für befristet angestellte, promovierte Nachwuchswissenschaftler:innen, im Fall ihrer erfolgreichen Qualifizierung eine Anschlusszusage durch die Universität für eine unbefristete Beschäftigung zu erhalten, ist somit nach

5 Vgl. BVerfG Urt. v. 29.05.1973 - 1 BvR 424/71, 1, 1 BvR 325/72.

6 BVerfG Urt. v. 29.05.1973 - 1 BvR 424/71, 1 BvR 325/72.

7 BVerfG Urt. v. 29.05.1973 - 1 BvR 424/71, 1 BvR 325/72; BVerfG Beschl. v. 24.04.1996 - 1 BvR 712/86.

8 BVerfG Urt. v. 29.05.1973 - 1 BvR 424/71, 1 BvR 325/72.

9 BVerfG Urt. v. 25.06.2025 - 1 BvR 368/22 Rn. 22.

10 BVerfG Beschl. v. 24.04.1996 - 1 BvR 712/86.

11 BVerfG Urt. v. 25.06.2025 - 1 BvR 368/22 Rn. 22.

länger anhaltender Debatte endgültig gescheitert. Gravierende praktische Auswirkungen sind allerdings nicht zu erwarten, da die Anwendung der Norm durch den Berliner Gesetzgeber bereits seit dem Jahr 2022 ausgesetzt ist. Durch die klarstellende Entscheidung des BVerfG wird nun jedoch das Entstehen eines „Flickenteppichs" landesrechtlicher Einzelregelungen verhindert. Ob die einschlägige Thematik im Rahmen der bis Mitte 2026 durch die Bundesregierung angestrebten Reform des WissZeitVG Berücksichtigung finden wird, bleibt abzuwarten.

## 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