„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

8 / 2024
August 2024

Europäische Sandkästen für KI

Mit der KI-Verordnung regelt die EU erstmals die Erprobung und Entwicklung von KI unter realen Bedingungen

Wer den Schaden hat, braucht für den Ärger nicht zu sorgen

Ein Überblick über die schadensrechtlichen Leitlinien des EuGH nach Art. 82 DSGVO

Telemedien out, Digitale Dienste in!

Zur Bedeutung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und des reformierten Telekommunikationsgesetzes für Hochschulen

Kurzbeitrag: The floor is yours, Bundesnetzagentur

Die Bundesnetzagentur ist nun zentrale Anlaufstelle für Aufsicht und Durchsetzung des neuen Rechtsrahmens für digitale Dienste

Europäische Sandkästen für KI

Mit der KI-Verordnung regelt die EU erstmals die Erprobung und Entwicklung von KI unter realen Bedingungen

von Philipp Schöbel, Berlin

Die KI-Verordnung wird neben einer Reihe von Regelungen zur Risikominimierung auch gesetzgeberische Instrumente zur Innovationsförderung enthalten. Die wichtigsten dieser Instrumente sind die sogenannten „regulatory sandboxes" – im Deutschen auch „KI-Reallabore" genannt.

I. Die KI-Verordnung und die Wissenschaftsfreiheit

Die KI-Verordnung (KI-VO) wird voraussichtlich im Juli in Kraft treten und soll ab 2027 weitestgehend gelten. Sie soll Innovation fördern, die Freiheit der Wissenschaft respektieren und die Forschungs- und Entwicklungstätigkeit fördern. Von ihrem Anwendungsbereich ausgenommen sind sowohl Forschung mit KI als auch Forschung an KI: Erstens erfasst die Verordnung nicht KI-Systeme oder KI-Modelle, die allein zum Zweck der wissenschaftlichen Forschung entwickelt und eingesetzt werden. Das Gleiche gilt zweitens für Forschungs-, Test- und Entwicklungstätigkeiten, die stattfinden, bevor ein KI-System auf den Markt gebracht oder eingesetzt wird – es sei denn, sie werden unter realen Bedingungen durchgeführt, also „in der echten Welt". Die Ausnahmen für die Forschung mit und an KI gelten nur für die Vorschriften der KI-VO und nicht für andere europäische Rechtsakte.

Die Verordnung ermöglicht es, KI-Systeme unter realen Bedingungen in sogenannten „regulatory sandboxes" (KI-Reallaboren) zu testen und zu entwickeln. Damit wirkt sich die KI-VO direkt auf die Arbeit von Wissenschaftler:innen aus. Der europäische Gesetzgeber betont, dass jede Forschungstätigkeit im Einklang mit anerkannten ethischen und professionellen Standards für wissenschaftliche Forschung und im Einklang mit dem sonstigen geltenden EU-Recht durchgeführt werden sollte.[1]

II. „Regulatory Sandboxes": Was sind KI-Reallabore?

Reallabore sind keine Eigenart der KI-VO. Sie sind aus der Regulierung von Finanzwesen, Luftfahrt, Verkehr und Energiewirtschaft bekannt.[2] In Deutschland hat das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ein Konzept für ein Reallabore-Gesetz vorgestellt.[3] Der Konsultationsprozess ist inzwischen beendet.[4] Ein offizieller Gesetzesentwurf wurde bisher nicht veröffentlicht.

Obwohl der Gesetzgeber das regulatorische Instrument breit einsetzt, fehlt bislang eine einheitliche Definition. Ähnliche

1 Vgl. Erwägungsgrund 25 KI-VO.

2 Rat der Europäischen Union, Schlussfolgerungen des Rates zu Reallaboren und Experimentierklauseln als Instrumente für einen innovationsfreundlichen, zukunftssicheren und resilienten Rechtsrahmen zur Bewältigung disruptiver Herausforderungen im digitalen Zeitalter, 16. November 2020, S. 3, abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-13026-2020-INIT/de/pdf (zuletzt abgerufen am 10.07.2024).

3 BMWK, Neue Räume, um Innovationen zu erproben - Konzept für ein Reallabore-Gesetz, 2021, abrufbar unter: https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/konzept-fur-ein-reallabore-gesetz.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 10.07.2024).

4 BMWK, Pressemitteilung vom 10. Juli 2023, abrufbar unter: https://www.bmwk.de/Redaktion/DE/Textsammlungen/Digitale-Welt/reallabore-konsultation.html (zuletzt abgerufen am 10.07.2024).

Konzepte sind etwa Living Labs, Innovationslabore und Realexperimente.[5] Der Rat der Europäischen Union versteht unter Reallaboren einen zeitlich und räumlich begrenzten Testraum, in dem strukturierte Bedingungen für Experimente und Entwicklung unter regulatorischer Aufsicht geschaffen werden.[6]

Die KI-VO orientiert sich an diesem Verständnis und definiert ein KI-Reallabor als einen von der zuständigen nationalen Behörde eingerichteten kontrollierten Rahmen. Dieser Versuchsrahmen soll es Anbieter:innen[7] ermöglichen, ein innovatives KI-System gemäß einem vorher vereinbarten Plan für eine begrenzte Zeit unter behördlicher Aufsicht zu entwickeln, zu trainieren, zu validieren und gegebenenfalls unter realen Bedingungen zu testen. In einem solchen vereinbarten Plan müssen die Anbieter:innen in Zusammenarbeit mit der zuständigen Behörde Folgendes gemeinsam festlegen:

- Ziele,
- Bedingungen,
- Zeitrahmen,
- Methode
- und Anforderungen an die im Reallabor durchgeführten Tätigkeiten.

Für die konkrete Umsetzung von KI-Reallaboren belässt die KI-VO den Akteuren einen weiten Gestaltungsspielraum: KI-Reallabore können unterschiedlich konzipiert sein; die KI-VO gibt keine „one-size-fits-all"-Lösung vor. Das KI-Reallabor sowie die zu entwickelnden Anwendungen und Produkte können physischer, digitaler oder hybrider Natur sein.

III. Ziele der KI-Reallabore

Der Gesetzgeber geht von der Prämisse aus, dass KI eine sich rasch entwickelnde Technologiefamilie ist, die eine regulatorische Aufsicht erfordert. Die Verordnung adressiert bei der Einrichtung von KI-Reallaboren Anbieter:innen von KI. Anbieter:innen sind die Personen, die ein KI-System entwickeln oder entwickeln lassen und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringen oder Betrieb nehmen.

KI-Reallabore sollen Innovation und Wettbewerbsfähigkeit fördern. Zugleich soll die kontrollierte Versuchs- und Testumgebung für die Entwicklungsphase sicherstellen, dass die entwickelte KI die rechtlichen Anforderungen der KI-VO und anderer einschlägiger Rechtsvorschriften erfüllt. Für die Anbieter:innen soll der Prozess die Rechtssicherheit erhöhen. Die zuständigen Behörden sollen die Wirkungsweise von KI besser verstehen, um den Rechtsrahmen im Idealfall besser auf die praktischen Gegebenheiten zuzuschneiden. Zudem sollen Zusammenarbeit und Austausch bewährter Praktiken zwischen Behörden gefördert werden. Werden bei der Entwicklung und Erprobung von KI-Systemen erhebliche Risiken festgestellt, müssen Anbieter:innen angemessene Maßnahmen zur Risikominderung implementieren. Ist eine Risikominderung nicht möglich, muss der Entwicklungs- und Erprobungsprozess ausgesetzt werden.

IV. Aufbau und Struktur von KI-Reallaboren

Während der Entwicklung im Reallabor sind Anbieter:innen verpflichtet, mit der zuständigen Behörde zusammenzuarbeiten und ihren Anweisungen zu folgen. Die Behörde bietet Anleitung, Aufsicht und Unterstützung, insbesondere zu Fragen, die für die Anbieter:innen noch mit Rechtsunsicherheiten verbunden sind. Sie erstellt Leitfäden zu regulatorischen Erwartungen und zur Erfüllung der in der KI-VO festgelegten Anforderungen und Pflichten. Bereits vor der Einrichtung eines KI-Reallabors kann die Behörde Anbieter:innen an beratende Dienste verweisen. Zweck der Zusammenarbeit von Behörden und Anbieter:innen ist es, die rechtliche Konformität der KI sicherzustellen – nicht die technische Entwicklung. Die Behörde darf die forschende Tätigkeit der Anbieter:innen nicht übernehmen oder ersetzen.

Auf Anfrage der Anbieter:innen stellt die Behörde ihnen einen schriftlichen Nachweis für die im Reallabor erfolgreich

---

5 BMWK, BMWi-Strategie - Reallabore als Testräume für Innovation und Regulierung, 2018, S. 4, abrufbar unter: https://www.bmwk.de/Redaktion/DE/Downloads/S-T/strategiepapier-reallabore.pdf?__blob=publicationFile&v=10 (zuletzt abgerufen am 10.07.2024).

6 Rat der Europäischen Union, Schlussfolgerungen des Rates zu Reallaboren und Experimentierklauseln als Instrumente für einen innovationsfreundlichen, zukunftssicheren und resilienten Rechtsrahmen zur Bewältigung disruptiver Herausforderungen im digitalen Zeitalter, 16. November 2020, S. 4, abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-13026-2020-INIT/de/pdf (zuletzt abgerufen am 10.07.2024).

7 Zum Begriff Anbieter:innen weiter unten.

durchgeführten Tätigkeiten aus. Außerdem verfasst die Behörde einen Abschlussbericht. Darin beschreibt sie die im Reallabor durchgeführten Tätigkeiten, deren Ergebnisse und die gewonnenen Erkenntnisse im Detail. Dieser Bericht soll es den Anbieter:innen erleichtern, bestimmte nachgelagerte Verfahren der Produktsicherheit durchzuführen (dazu unten mehr).

Die KI-VO sieht vor, dass die Mitgliedstaaten den zuständigen Behörden ausreichende Mittel zur Verfügung stellen, damit diese wirksam und zeitnah Reallabore einrichten können. Die Europäische Kommission kann den nationalen Behörden technische Unterstützung, Beratung und andere Instrumente für die Einrichtung und den Betrieb von KI-Reallaboren bereitstellen. Zudem wird sie eine eigene Schnittstelle einrichten, die alle relevanten Informationen zu KI-Reallaboren enthält. Interessenträger können so mit den KI-Reallaboren interagieren und Anfragen an die zuständigen Behörden richten.

Reallabore müssen nicht auf einen Mitgliedstaat begrenzt sein. Behörden unterschiedlicher EU-Mitgliedstaaten können auch gemeinsam ein KI-Reallabor einrichten. Auch ansonsten können nationale Behörden zusammenarbeiten und dabei nationale oder europäische Akteure in ihre Arbeit einbeziehen. Zu diesen Akteuren zählen: Normungsorganisationen, notifizierte Stellen, Test- und Versuchseinrichtungen, Forschungs- und Versuchslabore, europäische digitale Innovationszentren sowie einschlägige Interessenträger und Organisationen der Zivilgesellschaft.

V. Vorteile der Entwicklung in einem KI-Reallabor

Der Zugang zu einem KI-Reallabor ist grundsätzlich kostenlos.[8] Für Anbieter:innen erhöht die Teilnahme die Rechtssicherheit. Sie dürfen davon ausgehen, dass ihr in Absprache mit der Behörde entwickeltes KI-System gesetzeskonform ist, und können die von der Behörde erstellten Unterlagen auch für andere Verfahren nutzen, um nachzuweisen, dass sie die Vorschriften der KI-VO einhalten. So müssen etwa Marktüberwachungsbehörden die Unterlagen bei einer Prüfung positiv berücksichtigen.

Hinzu kommt: Soweit die Anbieter:innen den spezifischen Plan und die Bedingungen für die Beteiligung am KI-Reallabor beachten und Anweisungen der zuständigen nationalen Behörden in gutem Glauben folgen, dürfen die Behörden keine Geldbußen wegen Verstößen gegen Vorgaben der KI-VO verhängen. Auch vor Bußgeldern wegen eines Verstoßes gegen andere europäische Vorschriften (zum Beispiel die DSGVO) sind sie geschützt, wenn die für die Überwachung des jeweiligen Rechtsakts zuständige Behörde aktiv an der Beaufsichtigung des KI-Systems im Reallabor beteiligt war und eine Anleitung für die Einhaltung der entsprechenden Vorschriften bereitgestellt hat, die die Anbieter:innen in gutem Glauben befolgt haben.

Zu beachten ist aber: Die Einhaltung dieser Vorgaben führt nicht zu einer Haftungsprivilegierung, wenn Dritte, die Schäden erlitten haben, die Anbieter:innen verklagen. Geschädigte können ihre Ansprüche nach dem Zivilrecht der Mitgliedstaaten (in Deutschland etwa nach den Vorschriften des Bürgerlichen Gesetzbuchs (BGB)) geltend machen.

VI. Anforderungen an KI-Reallabore

Nach der KI-VO ist die Kommission dafür zuständig, Durchführungsrechtsakte zu erlassen, um die Anforderungen an KI-Reallabore weiter zu konkretisieren. Sie sollen detaillierte Regelungen für Einrichtung, Entwicklung, Umsetzung, Betrieb und Beaufsichtigung der KI-Reallabore enthalten. Ziel ist es, Forschungs- und Versuchslabore, einzelne Forschende sowie andere wissenschaftliche Akteure in die KI-Reallabore einzubeziehen und bei ihrer Arbeit zu unterstützen.

Für die Verarbeitung personenbezogener Daten sieht die KI-VO Spezialregelungen vor. Für die Verwendung personenbezogener Daten, die für einen anderen Zweck als die Entwicklung des KI-Systems erhoben wurden, enthält die KI-VO einen neuen Erlaubnistatbestand. Dies ist notwendig, damit die Datenverarbeitung nicht gegen den Zweckbindungsgrundsatz der DSGVO verstößt und dadurch rechtswidrig ist. Damit der Erlaubnistatbestand greift, muss das KI-System einem der nachfolgenden Ziele dienen: der öffentlichen Sicherheit, der öffentlichen Gesundheit, dem Umweltschutz, der nachhaltigen Energie, der Sicherheit und Widerstandsfähigkeit von Verkehrssystemen, kritischen Infrastrukturen, der Effizienz und Qualität der öffentlichen Verwaltung und öffentlicher Dienste.

8 Behörden können lediglich die Erstattung außergewöhnlicher Kosten verlangen. Was konkret unter diesem Begriff zu verstehen ist, ist nicht geregelt.

Die Datenverarbeitung muss zudem erforderlich sein, um die Einhaltung der Anforderungen der KI-VO an Hochrisiko-KI-Systemen[9] sicherzustellen. Dazu gehören zum Beispiel die Einrichtung eines Risikomanagementsystems, die Einrichtung eines Qualitätsmanagementsystems, die vorgeschriebene technische Dokumentation, Transparenzvorkehrungen, Vorkehrungen für Robustheit und Cybersicherheit. Erforderlich ist die Verarbeitung dann, wenn sich die Einhaltung der rechtlichen Anforderungen nicht durch eine Verarbeitung anonymisierter, synthetischer oder sonstiger nicht personenbezogener Daten wirksam erfüllen lässt.

Anbieter:innen müssen wirksame Überwachungsmechanismen schaffen und einhalten, um zu beobachten, ob hohe Risiken für die Rechte und Freiheiten betroffener Personen bei Reallaborversuchen bestehen. Die verwendeten Daten müssen in einer funktional getrennten, isolierten und geschützten Datenverarbeitungsumgebung unter der Kontrolle der Anbieter:innen aufbewahrt werden. Sie sind durch technische und organisatorische Maßnahmen zu schützen; nur befugte Personen dürfen Zugriff haben. Personenbezogene Daten, die im Reallabor entstanden sind, dürfen nicht außerhalb des Reallabors weitergegeben werden. Sobald die Beteiligung an dem Reallabor endet, sind die Daten zu löschen.

VII. Behördliche Zuständigkeit in Deutschland

Bislang ist unklar, welche Behörde in Deutschland für die Einrichtung von KI-Reallaboren zuständig sein wird. Die Datenschutzkonferenz, also das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, hat sich dafür ausgesprochen, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) sowie die Landesdatenschutzbehörden als nationale Marktüberwachungsbehörden zu benennen.[10] Die Bündelung von Datenschutz- und KI-Aufsicht würde dazu führen, dass die Bürger:innen „es mit nur einer Aufsichtsbehörde“ zu tun hätten. Auch verfügen die Datenschutzaufsichtsbehörden über die einschlägige Fachkunde und die notwendige Unabhängigkeit und sind mit funktionierenden Kooperations- und Kohärenzmechanismen ausgestattet. Zudem sind sie für KI-Systeme, die personenbezogene Daten verwenden, ohnehin zuständig. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit fügt dem hinzu, dass sich Doppelstrukturen und Rechtsunsicherheiten vermeiden ließen.[11]

VIII. Alternative zu KI-Reallaboren nach der KI-VO

KI-Systeme können grundsätzlich auch außerhalb von KI-Reallaboren getestet werden. Für Tests von Hochrisiko-KI-Systemen unter realen Bedingungen gelten dafür aber bestimmte Regelungen. KI-Systeme mit einem geringeren Risiko müssen diese Anforderungen hingegen nicht erfüllen. Die Vorgaben für Tests von Hochrisiko-KI-Systemen unter realen Bedingungen ähneln denen von KI-Reallaboren. So müssen Anbieter:innen etwa einen Plan für den Test erstellen und bei der zuständigen Marktüberwachungsbehörde einreichen. Die Behörde hat den Test anhand des eingereichten Plans zu genehmigen. Der Test muss in einer dafür einzurichtenden EU-Datenbank registriert werden. Er darf nicht länger dauern, als zur Erfüllung seiner Zielsetzung notwendig ist. Regelmäßig ist die Dauer auf sechs Monate begrenzt und kann einmalig um sechs Monate verlängert werden. Die Personen, die am Test teilnehmen, müssen vor Testbeginn ihre informierte Zustimmung erteilen. Zudem ist eine qualifizierte Person mit der wirksamen Überwachung des Tests zu beauftragen.

Wenn im Testverlauf ein schwerwiegender Vorfall eintritt, müssen Anbieter:innen ihn den nationalen Marktüberwachungsbehörden melden und Sofortmaßnahmen zur Schadensbegrenzung einleiten. Andernfalls müssen sie den Test abbrechen oder jedenfalls die Entwicklung aussetzen, bis eine Schadensbegrenzung

9 Zur Erklärung der unterschiedlichen Risikokategorien bereits Rennert, One KIss is all it takes in DFN-Infobrief Recht 01/2023; Europäisches Parlament, KI-Gesetz: erste Regulierung der künstlichen Intelligenz, abrufbar unter: https://www.europarl.europa.eu/topics/de/article/20230601STO93804/ki-gesetz-erste-regulierung-der-kunstlichen-intelligenz (zuletzt abgerufen am 10.07.2024)..

10 DSK, Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 3. Mai 2024, Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO), abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf (zuletzt abgerufen am 10.07.2024).

11 Berliner Beauftragte für Datenschutz und Informationsfreiheit, Pressemitteilung vom 8. Mai 2024, abrufbar unter: https://www.datenschutz-berlin.de/pressemitteilung/datenschutzkonferenz-bezieht-position-nationale-zustaendigkeiten-fuer-die-verordnung-zur-kuenstlichen-intelligenz/ (zuletzt abgerufen am 10.07.2024).

stattgefunden hat. Für Schäden, die während der Tests unter realen Bedingungen entstehen, sind die Anbieter:innen grundsätzlich nach den zivilrechtlichen Gesetzen der Mitgliedstaaten (in Deutschland beispielsweise nach dem BGB) haftbar.

Wer den Schaden hat, braucht für den Ärger nicht zu sorgen

Ein Überblick über die schadensrechtlichen Leitlinien des EuGH nach Art. 82 DSGVO

Von Ole-Christian Tech, Münster

Die Österreichische Post AG trieb Handel mit personenbezogenen Daten und ordnete diesen mittels Algorithmen eine Affinität zu politischen Parteien in Österreich zu. Dem Betroffenen wurde eine hohe Affinität zur als rechtspopulistisch geltenden FPÖ zugeordnet, wodurch sich der Betroffene „verärgert und beleidigt" fühlte. Er klagte auf Ersatz des Schadens, der durch eine unter Verstoß gegen die Datenschutzgrundverordnung (DSGVO) erfolgte Datenverarbeitung verursacht worden ist. Das Verfahren gelangte dann letztlich im Wege der Vorlage zur Vorabentscheidung nach Art. 267 AEUV (Vertrag über die Arbeitsweise der Europäischen Union) vor den Europäischen Gerichtshof (EuGH).[1] Das Urteil beschäftigt sich auf den ersten Blick mit eher theoretischen, schadensrechtsdogmatischen Erwägungen. Bei der weiteren Lektüre des Falls zeigt sich jedoch die erhebliche praktische Bedeutung dieses Grundsatzurteils, welche auch die weitreichende Berichterstattung in den Fachmedien begründet. Weitere Entscheidungen zu ähnlich gelagerten Vorlagefragen zum Schadenersatzanspruch nach Art. 82 DSGVO haben sich daran orientiert, so etwa das EuGH-Urteil vom 14. Dezember 2023, C-340/21[2] und das EuGH-Urteil vom 11. April 2024, C 741/21.[3]

I. Sachverhalt

Ab 2017 sammelte die Österreichische Post Informationen über die politische Affinität der österreichischen Bevölkerung. Mit Hilfe eines Algorithmus, der verschiedene soziale und demografische Merkmale berücksichtigt, wurden „Zielgruppenadressen" definiert. Die so generierten Daten wurden an verschiedene Organisationen verkauft, um diesen die gezielte Zusendung von Werbung zu ermöglichen. Dem Betroffenen wurde so eine hohe Affinität zur Freiheitlichen Partei Österreichs (FPÖ) in Österreich zugeordnet. Die FPÖ wird dabei gemeinhin als rechtspopulistische Partei eingeordnet. Die Informationen über den Betroffenen wurden jedoch nicht an Dritte weitergegeben, aber der Betroffene, welcher der Verarbeitung seiner personenbezogenen Daten nicht zugestimmt hatte, fühlte sich dadurch, dass ihm eine Affinität zu der Partei zugeschrieben wurde, beleidigt. Die Speicherung von Daten über seine mutmaßliche politische Einstellung durch die Österreichische Post AG habe bei ihm große Verärgerung, einen Vertrauensverlust und das Gefühl der Bloßstellung ausgelöst. Außer diesen vorübergehenden emotionalen Beeinträchtigungen bestand kein Schaden.

Vor diesem Hintergrund erhob der Betroffene des Ausgangsverfahrens beim Landesgericht für Zivilrechtssachen Wien Klage

1 Überblicksartig hierzu auch Voget, Kurzbeitrag: Nicht (un)erheblich?!, DFN-Infobrief Recht, 07/2023.

2 Hierzu auch Müller, Ich glaub, es hackt in: DFN-Infobrief Recht 04/2024.

3 Zu der hier aufgeworfenen Frage der Zurechnung des Verschuldens von Mitarbeitern siehe Müller, Ist das denn meine Schuld? in: DFN-Infobrief Recht 06/2024.

gegen die Österreichische Post auf

1. Unterlassung der Verarbeitung der fraglichen personenbezogenen Daten und
2. auf Zahlung von 1 000 Euro als Ersatz des ihm entstandenen immateriellen Schadens.

Nachdem der Betroffene mit seinem Unterlassungsbegehren obsiegte, blieb die Frage des Schadenersatzes offen, die der Oberste Gerichtshof im Wege eines Vorabentscheidungsersuchens an den EuGH stellte. Zur Begründung seines Vorabentscheidungsersuchens erläuterte das Gericht zunächst den Schadenersatzanspruch nach Art. 82 DSGVO unter Heranziehung der Erwägungsgründe der DSGVO. Zweitens war das vorlegende Gericht in Bezug auf die Bemessung des Schadenersatzes der Ansicht, dass der unionsrechtliche Effektivitätsgrundsatz nur begrenzte Wirkung entfalten könne, da die DSGVO bereits hohe Sanktionen für Verstöße gegen ihre Bestimmungen vorsehe[4] und es daher nicht erforderlich sei, zusätzlich einen Schadenersatz zuzusprechen, um die effektive Durchsetzung der DSGVO zu gewährleisten. Der aus diesem Grund geschuldete Schadenersatz müsse verhältnismäßig, wirksam und abschreckend sein, damit er eine Ausgleichsfunktion erfüllen könne, ohne einen dem Unionsrecht fremden Strafcharakter zu haben. Drittens stellt das vorlegende Gericht die Auffassung der Österreichischen Post in Frage, dass die Zuerkennung eines solchen Schadenersatzes von der Voraussetzung abhänge, dass die Verletzung des Schutzes personenbezogener Daten einen besonders hohen Schaden verursacht habe.

Unter diesen Umständen hat der Oberste Gerichtshof beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Erfordert der Zuspruch von Schadenersatz nach Art. 82 DSGVO neben einer Verletzung von Bestimmungen der DSGVO auch, dass der Kläger einen Schaden erlitten hat oder reicht bereits die Verletzung von Bestimmungen der DSGVO als solche für die Zuerkennung von Schadenersatz aus?
2. Bestehen für die Bemessung des Schadenersatzes neben den Grundsätzen der Effektivität und Äquivalenz weitere Vorgaben des Unionsrechts?
3. Ist die Auffassung mit dem Unionsrecht vereinbar, dass Voraussetzung für den Zuspruch immateriellen Schadens ist, dass eine Konsequenz oder Folge der Rechtsverletzung von zumindest einigem Gewicht vorliegt, die über den durch die Rechtsverletzung hervorgerufenen Ärger hinausgeht?

II. Das Urteil des EuGH

Zur ersten Frage

Der EuGH beginnt zunächst mit der Auslegung des Wortlauts von Art. 82 Abs. 1 DSGVO.[5] Dieser lautet: „(…) der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller **Schaden entstanden ist**“.[6] Das Erfordernis eines Schadens ist dabei bereits klar im Wortlaut angelegt.[7] Zudem wäre die gesonderte Erwähnung eines Schadens obsolet, wenn es lediglich auf einen Verstoß ankäme.[8]

Außerdem ergibt sich hieraus bereits ein Anspruchsaufbau, der aus drei kumulativen Voraussetzungen besteht: einem Verstoß gegen die DSGVO, einem Schaden und einer Kausalität zwischen dem DSGVO-Verstoß und dem entstandenen Schaden.[9] Hieraus ergibt sich auch ein weiteres, systematisches Argument für das Erfordernis eines Schadens: Wenn der Wortlaut ein dreistufiges Prüfungsschema vorsieht, wäre dies hinfällig, wenn das Ergebnis der Prüfung bereits durch das Vorliegen des zweiten Erfordernisses feststünde.[10]

---

4 Anmerkung des Autors: Gemeint sind die Bußgelder nach der DSGVO, welche von den Aufsichtsbehörden i.H.v bis zu 20 Mio. Euro oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes des vorherigen Geschäftsjahres verhängen können.

5 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 31.

6 Hervorhebung durch den Autor.

7 EuGH Urteil vom 4.Mai 2023, C-300/21, Rz. 32.

8 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 34.

9 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 32.

10 EuGH Urteil vom 4.Mai 2023, C-300/21, Rz. 34.

Anschließend bezieht das Gericht auch die Erwägungsgründe Nr. 75, 85 und 146 in die Auslegung mit ein.

Exkurs zu den Erwägungsgründen:
Die Erwägungsgründe zu europäischen Rechtsakten stehen am Anfang des Textes, vor dem normativen Teil und werden in der deutschen Sprachfassung eingeleitet mit den Worten: „In Erwägung nachstehender Gründe“. Hierauf folgt dann die Aufzählung der Erwägungsgründe.

Diese sind jedoch rechtlich nicht verbindlich und können weder herangezogen werden, um von den Bestimmungen des betreffenden Rechtsakts abzuweichen, noch, um diese Bestimmungen in einem Sinne auszulegen, der ihrem Wortlaut offensichtlich widerspricht.[11]

Dennoch sind die Erwägungsgründe als Ergänzung eine wichtige Erkenntnisquelle zur Interpretation und Anwendung des jeweiligen Rechtsakts und dürfen daher in einer umfassenden Untersuchung nicht fehlen.

So spricht Erwägungsgrund 146 etwa von „Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht“. Auch hieraus ergibt sich also das Erfordernis eines Schadens, der kausal („aufgrund“) auf der rechtswidrigen Verarbeitung entstanden ist, was auch das Erfordernis eines tatsächlich erlittenen Schadens impliziert.[12] In Erwägungsgrund 75 geht es um „[d]ie Risiken, [die] aus einer Verarbeitung personenbezogener Daten hervorgehen [können], die zu einem […] Schaden führen könnte[n]“ und in Erwägungsgrund 85 um eine „Verletzung des Schutzes personenbezogener Daten [die] einen […] Schaden […] nach sich ziehen [kann]“. Hieraus schließt das Gericht einerseits, dass aus einer rechtswidrigen Verarbeitung ein Schaden folgen kann, aber nicht muss, und andererseits, dass der Kausalzusammenhang zwischen DSGVO-Verstoß und Schaden eine notwendige Bedingung für den Schadenersatzanspruch nach Art. 82 DSGVO ist.[13]

Zudem führt der EuGH auch systematische Gründe für das Erfordernis eines Schadens an. So verweist das Gericht etwa auf die Art. 77 und 78 DSGVO (Rechte des Betroffenen gegenüber den Aufsichtsbehörden), welche gerade keinen Schaden, sondern nur einen Verstoß als Voraussetzung haben.[14] Hieraus ergibt sich der Umkehrschluss, dass ein Schaden dann eine notwendige Voraussetzung ist, wenn dieser im Wortlaut genannt wird. Letztlich bestätige dies auch der Vergleich zu den Bußgeldvorschriften nach Art. 83 und Art. 84 DSGVO.[15] Diese verfolgen einen Strafzweck und sollen somit bereits das rechtswidrige Verhalten unterbinden. Hierfür ist das Erfordernis eines erlittenen Schadens nicht erforderlich, sodass dieser nicht im Normwortlaut auftaucht. Der Zweck des Schadenersatzregimes ist jedoch vorrangig die Kompensation eines erlittenen Schadens, sodass hier - anders als im reinen Sanktionsregime - ein solcher Schaden erforderlich wird.

Somit kommt der EuGH im Ergebnis zu dem Schluss, „dass der bloße Verstoß gegen die Bestimmungen dieser Verordnung nicht ausreicht, um einen Schadenersatzanspruch zu begründen.“[16]

Zur zweiten Frage

Generalanwalt Sánchez-Bordona hatte hierzu in seinen Schlussanträgen die bis dahin noch nicht gestellte Frage aufgeworfen, inwiefern Art. 82 Abs. 1 DSGVO auch die Verhängung von Strafschadenersatz voraussetzt.[17] Diese Frage hat der EuGH in die Beantwortung der zweiten Frage aufgenommen.

Zunächst aber zu den Grundsätzen der Effektivität und Äquivalenz: Da es kein gemeineuropäisches Schadensrecht gibt, richtet sich die Festsetzung des Schadensersatzes nach den Vorschriften der einzelnen Mitgliedstaaten. Damit hierdurch aber das Unionsrecht nicht unterlaufen wird, indem zum Beispiel ein Mitgliedstaat sehr restriktiv bei der Festsetzung der Höhe vorgeht oder sehr kurze Verjährungsfristen setzt, müssen die Grundsätze der Effektivität und Äquivalenz beachtet werden.

11 Genau so: EuGH Urteil vom 19. Juni 2014, C-345/13, Rz. 31.

12 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 37.

13 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 37.

14 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 39.

15 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 40.

16 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 42.

17 Schlussanträge des Generalanwalts Manuel Campos Sánchez-Bordona vom 6. Oktober 2022, C-300/21 Rz. 35 ff.

Exkurs Äquivalenzgrundsatz und Effektivitätsgrundsatz:
Der Äquivalenzgrundsatz (teils auch Gleichwertigkeitsgrundsatz) greift in Fällen, in denen das Unionsrecht kein eigenes Rechtsregime für den Vollzug seiner Regeln beinhaltet, sodass das nationale Recht des jeweiligen Mitgliedstaats den Vollzug bestimmt. Damit dann aber kein Auseinanderklaffen der Rechtslage innerhalb der EU auf der Vollzugsebene entsteht und dadurch das Ziel der Harmonisierung (Angleichung der Rechtslage) unterlaufen wird, verlangt der Äquivalenzgrundsatz, dass die nationalen Regeln für den Vollzug von Unionsrecht die gleichen sein müssen, wie die für das nationale Recht.[18]

Im Kontext des Schadensrechts heißt das, dass der Gläubiger bei einem auf Unionsrecht basierenden Schadenersatzanspruch keine schlechtere Rechtsposition haben darf als bei einem auf nationalem Recht basierendem Anspruch.[19]

Der Effektivitätsgrundsatz (auch frz. effet utile) verlangt die hinreichend effektive Durchsetzung des Unionsrechts. Normativ folgt er aus Art. 4 Abs. 3 des Vertrags über die Europäische Union (EUV) und wird in Art. 197 Abs. 1 AEUV explizit benannt. [20]

Inhaltlich folgt hieraus, dass Unionsrecht in allen nationalen Rechtsordnungen möglichst wirksam umgesetzt werden muss, sodass Tragweite und Wirksamkeit der Harmonisierung nicht unterlaufen werden.

In der Praxis hat das zu Folge, dass nationale Vorschriften oder Rechtsgrundsätze bei der Anwendung von Unionsrecht nicht angewendet werden dürfen, wenn hierdurch eine effektive Rechtsdurchsetzung gefährdet würde. Das kann zum Beispiel Verjährungsvorschriften oder sehr restriktive Grundsätze zu bestimmten Schadenspositionen betreffen. Hieraus entstehende Rechtslücken sind dann etwa durch Analogien oder die Anwendung allgemeiner Rechtsgrundsätze zu überbrücken.[21]

Bezüglich des Äquivalenzgrundsatzes hatte der EuGH in dieser Hinsicht keine Bedenken am Vollzug durch das österreichische Recht.[22] Mit anderen Worten wurde der Schadenersatzanspruch aus Art. 82 Abs. 1 DSGVO also genauso behandelt wie andere Schadenersatzansprüche nach österreichischem Recht.

Im Zusammenhang mit dem Effektivitätsgrundsatz hingegen verlangt Erwägungsgrund 146 der DSGVO, dass ein „vollständige(r) und wirksame(r) Schadenersatz für den erlittenen Schaden“ geleistet werden muss.[23] Der EuGH schließt sich hierbei der Auffassung des Generalanwalts dahingehend an, dass es für einen solchen Schadenersatzanspruch lediglich notwendig ist, den „aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen, ohne dass ein solcher vollumfänglicher Ausgleich die Verhängung von Strafschadensersatz erfordert“.[24] Dahinter steckt letztendlich der bereits aus dem deutschen Schadensrecht bekannte Grundsatz der Totalreparation, wonach der Schädiger den gesamten Schaden zu ersetzen hat, unabhängig vom Grad des Verschuldens, seines finanziellen Leistungsvermögens oder etwaigen Billigkeitserwägungen.[25]

Einen darüber hinausgehenden Strafschadenersatz erfordert die DSGVO hingegen nicht.[26]

Exkurs Strafschadenersatz:
Strafschadenersatz (engl. punitive damages) sind ein vorrangig im anglo-amerikanischen Common Law genutztes Instrument,

18 Classen in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 80. EL Mai 2023, AEUV Art. 197 Rn. 23; Zum Ursprung des Rechtsgrundsatzes siehe EuGH Urteil vom 21. September 1983, Rs. 205/82, Rz. 23.

19 Ähnlich zum unionsrechtlichen Staatshaftungsanspruch: Thomas in: BeckOGK BGB § 839 Rn. 932.

20 Zum Ursprung des Rechtsgrundsatzes siehe EuGH Urteil vom 21.September 1983, Rs. 205/82, Rz. 22.

21 Classen in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 80. EL Mai 2023, AEUV Art. 197 Rn. 27.

22 EuGH Urteil vom 4.Mai 2023, C-300/21, Rz. 55.

23 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 57.

24 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 58.

25 Zur Totalreparation näher: Magnus in: Dauner-Lieb/Langen, BGB Schuldrecht 4. Auflage 2021 Rn. 30.

26 EuGH Urteil vom 04. Mai 2023, C-300/21, Rz. 59.

um neben dem Zweck der Kompensation auch die Zwecke der Bestrafung und Abschreckung zu erfüllen.[27] Hierbei können die punitive damages je nach Ausgestaltung dem Geschädigten, dem Staat oder anteilig beiden zugesprochen werden.

Sinn der punitive damages ist dabei, dass dem Fehlverhalten des Schädigers ein im Voraus kaum abschätzbarer Haftungsfall droht, sodass dieser etwaige Haftungsrisiken nicht in seine eigene Kalkulation mit aufnehmen und somit einen kalkulierten Rechtsbruch begehen kann.

Ein Strafschadenersatz könnte daher durchaus einen Beitrag zur effektiven Rechtsdurchsetzung der DSGVO leisten, ist jedoch nach der Auffassung des EuGH nicht erforderlich, da das bestehende System der Bußgelder und Aufsichtsbehörden in den Mitgliedstaaten diese Funktion ausreichend abdeckt. Damit ist jedoch nicht der Umkehrschluss verbunden, dass Strafschadenersatz für Schadenersatz wegen Verstößen gegen die DSGVO generell unzulässig wäre. Vielmehr dürfte es hier – auch mit Blick auf den Äquivalenzgrundsatz – auf die bestehende Praxis in den jeweiligen Mitgliedstaaten ankommen. Verhängen die Gerichte dort nach ihrem nationalen Recht Strafschadenersatz, können sie diesen auch nach der DSGVO zusprechen.

Zur dritten Frage

Die dritte Frage betrifft vereinfacht eine sog. Erheblichkeitsschwelle. Eine solche stellt eine Ausnahme zum eben vorgestellten Grundsatz der Totalreparation dar und findet sich zum Beispiel im deutschen Recht bei der Ersatzfähigkeit von immateriellen Schäden (so wie im hier zugrunde liegenden Verfahren). Dabei wird verlangt, dass ein Schaden oberhalb einer Bagatellschwelle liegt, soweit es den Umständen nach nicht der Billigkeit entspräche, den immateriellen Schaden durch ein Schmerzensgeld auszugleichen.[28] Der EuGH erinnert hier zunächst noch einmal daran, dass der Begriff des „Schadens", insbesondere des „immateriellen" Schadens nach Art. 82 DSGVO unionsrechtlich autonom ausgelegt werden muss.[29]

In Art. 82 Abs. 1 DSGVO ist der immaterielle Schaden explizit genannt, jedoch ohne jede Erwähnung einer Erheblichkeitsschwelle.[30]Somit spricht eine reine Wortlautauslegung bereits gegen die Erheblichkeitsschwelle. Zudem führt das Gericht auch hier den Erwägungsgrund 146 an. Nach diesem solle „[d]er Begriff des Schadens […] im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht".[31] Hierzu stünde eine Erheblichkeitsschwelle im Widerspruch. Auch eine teleologische Auslegung mit Blick auf den in Erwägungsgrund 146 geforderten Grundsatz der Totalreparation spricht gegen eine Erheblichkeitsschwelle.[32]

Außerdem gehört es zu den Zielen der DSGVO, einen EU-weit einheitlichen und hohen Standard beim Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten und für eine unionsweit gleichmäßige und einheitliche Anwendung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Betroffenen bei der Verarbeitung personenbezogener Daten zu sorgen.[33] Mit anderen Worten würde die Vollharmonisierung des Datenschutzrechts in der EU nicht gelingen, wenn einzelne Mitgliedstaaten eine Erheblichkeitsschwelle anwenden und andere nicht, sodass das Schutzniveau in den Mitgliedstaaten auseinanderdriften würde und womöglich auch der Binnenmarkt darunter leiden könnte. Dahinter steckt nicht zuletzt die Sorge, dass besonders restriktive Mitgliedstaaten attraktiver für datenverarbeitende Unternehmen würden und somit Anreize schaffen, sich in Ländern mit einem geringeren Haftungsrisiko für die Verantwortlichen niederzulassen. Hierdurch könnte ein Unterbietungswettbewerb im Schutzniveau für den Betroffenen entstehen, der die Ziele der DSGVO konterkariert und den gemeinsamen Binnenmarkt in Frage stellt.

---

27 Stempflein: Münchener Anwaltshandbuch Versicherungsrecht, Höra/Schubach 5. Auflage 2022 § 37 Rn. 94

28 Pardey in: Geigel, Haftpflichtprozess, 28. Auflage 2020 Kapitel 6 Rn. 14.

29 EuGH Urteil vom 04. Mai 2023, C-300/21, Rz. 44; Zur Auslegung von Unionsrecht siehe näher Wegener in: Calliess/Ruffert, EUV/AEUV 6. Auflage 2022, Art. 19 EUV Rn. 28ff.

30 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 45.

31 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 46.

32 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 47.

33 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 48.

Der EuGH stellt also im Ergebnis klar, dass eine Erheblichkeitsschwelle im Rahmen des Schadenersatzanspruchs nach Art. 82 Abs. 1 DSGVO mit der DSGVO unvereinbar ist.[34] Damit können selbst Bagatellschäden zu einem Anspruch des Betroffenen führen, solange er nur in der Lage ist, überhaupt einen Schaden als Resultat eines Verstoßes gegen die DSGVO nachzuweisen.

III. Fazit und Auswirkungen auf wissenschaftliche Einrichtungen

Zusammenfassend kann man also zu der Leitentscheidung des EuGH vom 4. Mai 2023, C-300/21 festhalten, dass:

1. Ein Schaden ein konstitutives Element für den Schadenersatzanspruch nach Art. 82 Abs. 1 DSGVO ist;
2. Neben den Grundsätzen der Effektivität und Äquivalenz keine weitergehenden Anforderungen an den Vollzug des Art. 82 DSGVO in den Mitgliedstaaten gestellt werden, insbesondere die Verhängung von Strafschadenersatz unionsrechtlich nicht erforderlich ist;
3. Eine Erheblichkeitsschwelle in Zusammenhang mit dem Schadenersatzanspruch nach Art. 82 Abs. 1 DSGVO unionsrechtswidrig ist.

Diese Grundsätze wurden später nochmals durch das EuGH-Urteil vom 14. Dezember 2023, C-340/21 und das EuGH-Urteil 11. April 2024, C-741/21 dergestalt bestätigt und konkretisiert, dass:

4. Auch ein Kontrollverlust über personenbezogenen Daten einen immateriellen Schaden darstellt;
5. Die Befürchtung, dass personenbezogene Daten durch Dritte missbräuchlich verwendet werden könnten, einen immateriellen Schaden darstellt;
6. Die Bemessung der Höhe des Schadenersatzanspruchs sich nicht an den Kriterien für die Bußgeldhöhe nach Art. 83 DSGVO orientiert;
7. Der Verantwortliche grundsätzlich auch für das Verschulden seiner Mitarbeiter haftet, er muss vielmehr sicherstellen, dass unterstellte Personen weisungsgemäß handeln;
8. Eine Schadenersatzpflicht nach Art. 82 DSGVO auch für unbefugte Offenlegung von personenbezogenen Daten durch einen Hackerangriff greift, sofern der Verantwortliche sich nicht exkulpieren kann.

Wissenschaftliche Einrichtungen verarbeiten große Mengen an Daten von Einzelpersonen und sind daher einem erhöhten Haftungsrisiko ausgesetzt. Öffentliche Stellen sind – jedenfalls dann, wenn sie nicht am Wettbewerb teilnehmen – in der Regel von Bußgeldern nach Art. 83 DSGVO ausgenommen.[35] Für Schadenersatzansprüche nach Art. 82 DSGVO hingegen besteht eine solche Ausnahme nicht, sodass für öffentliche Stellen wie Hochschulen, Behörden und Forschungseinrichtungen die Frage der Schadenersatzpflicht ungleich relevanter wird.[36]

Dass diese Leitlinien in der Praxis nicht immer leicht handhabbar sind, zeigt auch ein Blick auf die instanzgerichtlichen Entscheidungen in den Mitgliedstaaten. Insbesondere die Unterscheidung zwischen legitimen Interessen an dem Ersatz entstandener immaterieller Schäden einerseits und den Schadenersatzklagen als Geschäftsmodell andererseits stellt Gerichte hier vor Probleme. Während Gerichte sehr selten rechtsmissbräuchliches Klageverhalten erkennen,[37] zeichnet sich vielmehr der Trend zur Zusprechung von Kleinstbeträgen ab. Hierdurch kann sich ein vermeintliches Geschäftsmodell unter der prozessualen Kostentragungsregel schnell zu einem Nullsummenspiel entwickeln. [38]

---

34 EuGH Urteil vom 4. Mai 2023, C-300/21, Rz. 51, noch einmal betont in EuGH, Urteil vom 14. Dezember 2023, C-456/22 Rz. 23.

35 So zum Beispiel § 32 DSG NRW i.V.m. § 5 Abs. 5 Nr. 1 bis 4 DSG NRW.

36 Vgl. auch Müller, Ich glaub, es hackt in: DFN-Infobrief Recht 04/2024.

37 So jüngst aber das AG Augsburg, (Urteil vom 27.06.2024, Az.18 C 3234/23).

38 Siehe hierzu Tech, Wie gewonnen, so zerronnen in: DFN-Infobrief Recht, 04/2024.

Telemedien out, Digitale Dienste in!

Zur Bedeutung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und des reformierten Telekommunikationsgesetzes für Hochschulen

Von Anna Maria Yang-Jacobi, Berlin

Mit dem Inkrafttreten des Digitale-Dienste-Gesetzes (DDG) zum 14. Mai 2024 wurde das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) zum Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG). Die Namensänderung gibt Anlass sowohl das „neue" TDDDG als auch das Telekommunikationsgesetz (TKG) nach der umfassenden Novellierung von 2021 genauer zu betrachten. Einige Veränderungen sind für Hochschulen von Bedeutung.

I. Namensänderung vom TTDSG zum TDDDG

Der Gesetzgeber schuf 1996 mit dem TKG ein umfangreiches Gesetz zur Regulierung des Telekommunikationsmarktes in Deutschland. Einzelne Bestimmungen des TKG hielten jedoch gerichtlichen Überprüfungen nicht stand. Zudem gab es im Laufe der Jahre auch europarechtliche Vorgaben, die der Gesetzgeber in nationales Recht umsetzen musste. 2021 wurden Regelungen, die bislang im TKG und Telemedien-Gesetz (TMG) zu finden waren, angepasst. Dabei lagerte der Gesetzgeber Bestimmungen zum Datenschutz aus dem TKG und TMG in ein eigenes Gesetz – das TTDSG – aus.

Das TTDSG verblieb jedoch nicht lange in seiner Form von 2021. Grund dafür war der seit dem 17. Februar 2024 geltende Digital Services Act (DSA).[1] Mit dem DSA schufen die EU-Staaten einen einheitlichen Rechtsrahmen, um sicherzustellen, dass sich Nutzende von Online-Plattformen und Suchmaschinen in einem sicheren digitalen Umfeld bewegen können. In Deutschland wurde im Rahmen des Inkrafttretens des DSA zusätzlich ein Begleitgesetz eingeführt – das DDG. Der Zweck des Begleitgesetzes besteht darin, die Regelungen des DSA im nationalen Recht auszuführen und die nationalen Aufsichts- und Durchsetzungskompetenzen zuzuweisen.[2] Das Netzwerkdurchsetzungsgesetz von 2017 und die verbliebenen Regelungen im TMG wurden in der Folge durch den DSA und das DDG ersetzt.

Die Hauptveränderung für das TTDSG ist eine rein namentliche Änderung. Der Begriff „Telemedien" wurde durch „digitale Dienste"[3] ersetzt. Digitale Dienste sind nach § 1 DDG Dienstleistungen der Informationsgesellschaft. Durch die Verabschiedung des DDG waren zahlreiche Umbenennungen in anderen Gesetzen notwendig, die zuvor auf Telemedien verwiesen. So wurde auch das TTDSG zum TDDDG. Die nun vollständige Ablösung des TMG durch das DDG und die Umbenennung des TTDSG zum TDDDG haben auch Folgen für Hochschulen. Dabei geht es speziell um die Webseiten der Hochschulen.

Zunächst ist eine Veränderung im Impressum der Webseite erforderlich. Früher war die Impressumspflicht auf Webseiten im TMG geregelt. Aus § 5 TMG wurde nun § 5 DDG. Der Inhalt der Vorschrift ist allerdings identisch mit der Version von 2021. Sofern bisher ein Impressum bereitgestellt und im Impressum auf die Pflichtangabe nach § 5 TMG verwiesen wurde, ist diese Angabe in § 5 DDG zu ändern. Zusätzlich ist allerdings darauf

1 Vgl. zum DSA, Rennert, Brüssel reguliert das schon, DFN-Infobrief Recht 06/2022; Gielen, Digital Services Act: Das Plattformgrundgesetz?, DFN-Infobrief Recht 03/2021.

2 Zur neuen Koordinierungsstelle für digitale Dienste: von Bernuth, Kurzbeitrag: Bundesnetzagentur wacht über Einhaltung des DSA, DFN-Infobrief Recht 08/2024.

3 Vgl. zum Begriff, Mc Grath, Das Dilemma der Digitalen Dienste, DFN-Infobrief Recht 03/2021.

hinzuweisen, dass keine Pflicht von Webseitenbetreibern zur Nennung der gesetzlichen Grundlage im Impressum besteht. Vielmehr muss nur das Impressum als solches vorhanden sein. Um zukünftigen Entwicklungen der Vorschriften bereits vorab zu begegnen, könnte der namentliche Verweis auf § 5 DDG im Impressum auch vollständig entfernt werden.

Sofern in der Datenschutzerklärung bisher auf Vorschriften im TTDSG verwiesen wurde, ist auch hier eine Anpassung zum TDDDG notwendig.

Der weitere Anpassungsbedarf betrifft Verweise auf Cookies und die dazugehörigen Einwilligungsnormen. Ähnlich wie im ersten Fall besteht auch hier keine Pflicht, die rechtliche Grundlage zu nennen. Sofern allerdings auf § 25 TTDSG verwiesen wird, ist dieser Verweis durch § 25 TDDDG zu ersetzen. Wenn Webseiten nicht rechtskonform gestaltet sind, könnten Aufsichtsbehörden durch den veralteten Verweis aufmerksam werden und eine ausführlichere Kontrolle veranlassen.

II. Auslagerung des Datenschutzes im Jahr 2021

Für ein besseres Verständnis des TDDDG ist es notwendig, die Historie des Vorgänger-Gesetzes ab 2021 zu erläutern. Zunächst musste die europäische e-Privacy-Richtlinie in das nationale deutsche Recht umgesetzt werden. Das Ziel des damaligen TTDSG[4] war es sodann mehr Klarheit zwischen DSGVO, e-Privacy-Richtlinie, TMG und TKG zu schaffen. Die Vorschriften waren nach § 1 Abs. 3 Fall 1 TTDSG auf alle Unternehmen und Personen, die im Geltungsbereich dieses Gesetzes eine Niederlassung haben, anwendbar. Hochschulen in Deutschland mussten sich somit schon damals an die Vorgaben des TTDSG halten.

§§ 3 bis 18 TTDSG enthielten Vorschriften zur Privatsphäre der Telekommunikation (Fernmeldegeheimnis) und zum Schutz personenbezogener Daten (in Ergänzung zur DSGVO). Diese adressierten vor allem Anbieter von Telekommunikationsdiensten. §§ 19-26 TTDSG betrafen wiederum den Datenschutz bei Telemedien und Endeinrichtungen. Telemedien im Sinne des TMG waren alle Datenangebote von Texten, Zeichen, Bildern oder Tönen, die gerade keine Telekommunikationsdienste darstellen.[5] Dazu gehörten auch Homepages beziehungsweise Webseiten als Ganze. Im Folgenden werden die für Hochschulen relevantesten Regelungen aus den jeweiligen Bereichen behandelt. Die Vorschriften zum Fernmeldegeheimnis, dem Datenschutz und den Cookie-Regelungen bleiben durch die Umbenennung inhaltlich unverändert. Auch hier gilt, dass nur der Name des Gesetzes verändert wurde. Nachstehend wird zur leichteren Lesbarkeit bei Regelungen die nun gültige Gesetzesbezeichnung des TDDDG verwendet.

1. Das Fernmeldegeheimnis

Das Fernmeldegeheimnis ist in Art. 10 Abs. 1 Grundgesetz (GG) verankert. Es schützt den Inhalt sowie die Verkehrsdaten der Telekommunikation, also, wer wann mit wem wie lange kommuniziert hat. Der gesamte technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen ist davon umfasst. § 3 TDDDG, als Nachfolgenorm des Fernmeldegeheimnisses nach § 88 TKG, stellt die einfachgesetzliche Ausprägung des Art. 10 Abs. 1 GG dar. Die Grundrechte gelten unmittelbar nur im Verhältnis Staat-Bürger. Daher ist eine einfachgesetzliche Umsetzung im Verhältnis Bürger-Bürger notwendig. § 3 TDDDG enthält dabei nur das Verbot, das Fernmeldegeheimnis zu verletzen. Pflichten zum aktiven Schutz des Fernmeldegeheimnisses ergeben sich unmittelbar aus § 165 Abs. 1 TKG. Eine Verletzung des Fernmeldegeheimnisses wird über § 206 Strafgesetzbuch auch strafrechtlich sanktioniert.

Für Hochschulen relevant ist die Frage, ob diese in ihrer Funktion als Arbeitgebende auch zur Wahrung des Fernmeldegeheimnisses verpflichtet sind. Sie könnten von § 3 Abs. 2 Nr. 2 TDDDG erfasst werden, indem sie an den geschäftsmäßig angebotenen Telekommunikationsdiensten mitwirken. Für eine Geschäftsmäßigkeit ist dabei keine Gewinnerzielungsabsicht erforderlich. Vielmehr genügt ein auf Dauer angelegtes Angebot, das für Dritte erbracht wird. Der Drittbezug wird angenommen, wenn der Arbeitgebende eine private Nutzung der Systeme erlaubt. Nach dem ursprünglichen Sinn des Fernmeldegeheimnisses sollten die an der Kommunikation Beteiligten so behandelt werden wie bei einer Kommunikation ohne technische Hilfe. Sofern also

4 Vgl. vertiefend, John, TTDSG – Die Profis in spe, DFN-Infobrief Recht 05/2021.

5 Bundeszentrale für Kinder- und Jugendmedienschutz, https://www.bzkj.de/bzkj/indizierung/was-bewirkt-die-indizierung/telemedien/telemedium-175562 (zuletzt abgerufen am 10.7.2024).

ein Zugriff auf die Kommunikation möglich ist, ist die Kommunikation zu schützen. Eine Hochschule als Arbeitgebende, die die Server und weitere IT-Dienste dauerhaft zur Verfügung stellt, ist in der Lage, auf die technischen Systeme zuzugreifen. So kann sie Kenntnis vom Inhalt der Kommunikation erlangen. Gerade bei einer erlaubten privaten Nutzung der Systeme fällt auch die Hochschule unter den Kreis der Verpflichteten nach § 3 Abs. 2 Nr. 2 TDDDG. Das Fernmeldegeheimnis ist somit grundsätzlich gerade bei erlaubter Privatnutzung zu wahren.

Mit Bezug zum Fernmeldegeheimnis wurde nach einer Entscheidung des Bundesgerichtshofs zum digitalen Nachlass § 4 TDDDG als Vorschrift in das TDDDG aufgenommen.[6] Hierdurch wird es Erben und anderen berechtigten Personen ermöglicht, Rechte des betroffenen Endnutzers gegenüber Anbietern von Telekommunikationsdiensten geltend zu machen. Sofern Erbende oder andere berechtigte Personen Zugriff auf E-Mail-Konten oder Konten in sozialen Medien oder andere Dienste der Telekommunikation einer verstorbenen Person begehren, liegt ausnahmsweise kein Verstoß des Fernmeldegeheimnisses vor. So schafft § 4 TDDDG zusätzliche Rechtssicherheit. Diese Regelung gilt bei Annahme der Bindung der Hochschulen an das Fernmeldegeheimnis auch für diese.
Außerdem nennenswert ist die Legitimation zur Verarbeitung von notwendigen (und abschließend aufgezählten) Verkehrsdaten nach § 9 Abs. 1 TDDDG. Verkehrsdaten werden bei der Verbindung automatisch erzeugt und elektronisch verarbeitet. Sofern keiner der Fälle in § 9 Abs. 1 S. 1 TDDDG vorliegt, sind die gespeicherten Verkehrsdaten gemäß § 9 Abs. 1 S. 2 TDDDG nach der Beendigung der Verbindung unverzüglich zu löschen.

2. Datenschutz, Cookies und PIMS

Für (mittlerweile sogenannte) Anbieter von digitalen Diensten schreibt § 19 TDDDG vor, dass bestimmte technische und organisatorische Vorkehrungen einzuhalten sind. Dazu gehören die jederzeitige Beendigungsmöglichkeit der Nutzung, die anonyme Nutzbarkeit und die Anzeige bei Weitervermittlung zu einem anderen digitalen Diensteanbieter. Diese Vorgaben sind auch von Hochschulen beim Betreiben von Webseiten zu erfüllen.

Die Regelungen in §§ 21 bis 24 TDDDG betreffen das Auskunftsverfahren bei Bestands- und Nutzungsdaten. Bestandsdaten sind in § 2 Abs. 2 Nr. 2 TDDDG als personenbezogene Daten, deren Verarbeitung zum Zweck der Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Anbieter und Nutzer der digitalen Dienste erforderlich sind, definiert. Nutzungsdaten sind nach § 2 Abs. 2 Nr. 3 TDDDG wiederum die personenbezogenen Daten, deren Verarbeitung erforderlich ist, um die Inanspruchnahme der digitalen Dienste zu ermöglichen. Diese Daten entstehen bei jeder Nutzung des Dienstes. Bezüglich Bestands- und Nutzungsdaten gilt, dass alle Personen, die geschäftsmäßig digitale Dienste erbringen, unter den Voraussetzungen der §§ 22 ff. TDDDG Auskünfte auf Verlangen öffentlicher Stellen erteilen müssen. Geschäftsmäßig bedeutet nach den Materialien zum Gesetzesentwurf der Vorgängernorm im TMG nur, dass es sich um eine planmäßige und dauerhafte Tätigkeit handeln muss. Hochschulen betreiben ihre Webseiten planmäßig und dauerhaft, weshalb diese sich auch an die Regelungen halten müssen. In den Normen werden allerdings Differenzierungen bzgl. der Art der Daten und der jeweiligen öffentlichen Stellen sowie weiterer Bedingungen gemacht. Dabei bilden die §§ 22 bis 24 TDDDG nur die erste Stufe der Berechtigung und müssen durch eine entsprechende Berechtigungsnorm der öffentlichen Stellen zur Auskunft ergänzt werden.

Das Speichern nicht-personenbezogener Informationen auf Endgeräten und Auslesen durch Akteure der Privatwirtschaft war in Deutschland vor der Einführung des damaligen TTDSG nicht reguliert. Das TTDSG regelte insbesondere die Erforderlichkeit von Cookies und ähnlicher Technologien neu.[7] Mit § 25 TDDDG, der ein grundsätzliches Einwilligungserfordernis unabhängig vom Personenbezug der Daten festlegt, wurde eine europarechtskonforme Umsetzung von Art. 5 Abs. 3 e-Privacy-Richtlinie geschaffen. Allerdings blieb nach Inkrafttreten des TTDSG die Frage der Einwilligungsbedürftigkeit gerade bei funktionalen Cookies weiterhin offen. Vorgaben zu Modalitäten der Einwilligung wurden auch nicht getroffen. Neu eingeführt wurde zudem § 26 Abs. 1 TDDDG, der eine Regelung zu Diensten zur Einwilligungsverwaltung, sogenannten Person Information Management-Systeme („PIMS“) enthält.[8] Eine Befolgungspflicht der PIMS-Dienste lässt sich aber nicht aus dem TDDDG ableiten.

---

6 Vgl. ausführlich zum § 4 TTDSG, Mc Grath, Geheim bis das Erbe uns scheidet, DFN-Infobrief Recht 06/2022.

7 Vgl. vertiefend zu den Cookie-Regelungen, John, Ein Tool, die Banner zu knechten, DFN-Infobrief Recht 01/2022.

8 Vgl. vertiefend zu den PIMS, John, Ein Tool, die Banner zu knechten, DFN-Infobrief Recht 01/2022. Solche PIMS sind auch als „Dienste für die gemeinsame Datennutzung“ im Data Governance Act angelegt.

Nur dieser kurze Ausschnitt und die allseits bekannten Erfahrungen mit der „Cookie-Flut“ zeigen bereits, dass die Neuerungen zu Cookies und PIMS von der Politik gut gemeint waren, aber teilweise nicht gut umgesetzt wurden.

III. Die Relevanz des TKG für Hochschulen

Bis zum Jahr 2021 waren einige der bisher behandelten Vorschriften noch im TKG und TMG geregelt. Ziele der aktuellen Version des TKG sind, den Wettbewerb unter Telekommunikationsunternehmen zu regulieren, die Entwicklung neuer Infrastrukturen wie 5G-Netze zu fördern und den Netzzugang der Allgemeinheit zu fairen Bedingungen zu gewährleisten. Dabei gilt das Gesetz nach § 1 Abs. 2 TKG für alle Unternehmen oder Personen, die im Geltungsbereich dieses Gesetzes Telekommunikationsnetze oder -anlagen betreiben oder Telekommunikationsdienste erbringen. Die bekannten Telekommunikationsunternehmen im Bereich Festnetz, Mobilfunk und Internet liegen als Adressatenkreis nahe. Unumstritten stellen aber auch Hochschulen durch das Angebot von Telefonie, Internetzugängen sowie E-Mail-Diensten Telekommunikationsdienste im Sinne des § 3 Nr. 61 TKG bereit.

Für Hochschulen sind einzelne Regelungen des TKG von besonderer Relevanz. Erstens sind nach § 165 Abs. 1 TKG angemessene technische Vorkehrungen zum Schutz des Fernmeldegeheimnisses und zum Schutz von personenbezogenen Daten zu treffen.

Zweitens ist das manuelle Auskunftsverfahren gemäß § 174 Abs. 1, Abs. 6 TKG auch auf Hochschulen als Erbringer von Telekommunikationsdiensten anwendbar. So dürfen bereits erhobene Bestandsdaten zur Erfüllung von Auskunftspflichten verwendet werden. Bestandsdaten sind nach § 3 Nr. 6 TKG die Daten eines Endnutzenden, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertrags wie beispielsweise Name, Anschrift oder statische IP-Adressen wichtig sind.

Die Norm wurde nach einem Urteil des Bundesverfassungsgerichts (BVerfG)[9] inhaltlich an das sogenannte Doppeltürmodell angepasst. Das Doppeltürmodell stellt klar, dass bei Regelungen eines Datenaustauschs mit staatlichen Stellen zwischen der Datenübermittlung und dem Datenabruf zu unterscheiden ist: „Ein Datenaustausch vollzieht sich durch die einander korrespondierenden Eingriffe von Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen. Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten.“[10] § 174 Abs. 1 S. 1 TKG ist somit die Übermittlungsnorm, die Erbringer von Telekommunikationsdiensten zur Übermittlung der Daten berechtigt, aber gerade keine Befugnisnorm der Behörden zur Auskunft. Die Ermächtigung zum Auskunftsbegehren der Behörde muss sich aus anderen Fachgesetzen ergeben. Folglich hat die Fachbehörde selbst auf eine Rechtsgrundlage für ihr Auskunftsbegehren zu verweisen. § 174 Abs. 2 bis Abs. 5 TKG stellen ergänzend detaillierte Vorgaben zum Auskunftsverlangen dar. Nach § 174 Abs. 6 TKG sind die Daten bei berechtigtem Verlangen unverzüglich und vollständig zu übermitteln.

IV. Fazit

Das TTDSG wurde zum 14. Mai 2024 in das TDDDG umbenannt. Die Veränderung hat nur redaktionellen Charakter. Hochschulen sollten tätig werden, sofern das Impressum der Webseiten auf die Rechtsgrundlage des nun § 5 DDG, die Datenschutzerklärung auf Vorschriften des nun TDDDG oder die Cookie-Regelungen auf den nun § 25 TDDDG verweisen.

Insgesamt wurden die datenschutzrechtlichen Bestimmungen aus der e-Privacy-Richtlinie ab 2021 aus dem TKG und TMG in ein neues Gesetz, das heutige TDDDG, ausgelagert. Dort sind unter anderem Regelungen zum Fernmeldegeheimnis und datenschutzrechtliche Vorgaben enthalten. Einige juristische Fragen blieben auch mit Einführung des Gesetzes ungeklärt.

Bezogen auf das TKG sind für Hochschulen vor allem § 165 Abs. 1 TKG und § 174 Abs. 1, Abs. 6 TKG von Bedeutung. Auch Hochschulen sind bezogen auf das Fernmeldegeheimnis und im Rahmen des manuellen Auskunftsverfahrens verpflichtet beziehungsweise berechtigt.

Seit vielen Jahren bleibt offen, ob und wann die bereits seit 2017 geplante e-Privacy-Verordnung in der EU verabschiedet wird.

9 BVerfG, Beschluss v. 27.5.2020 – Az. 1 BvR 1873/13, 1 BvR 2618/13.

10 BVerfG, Beschluss v. 27.5.2020 – Az. 1 BvR 1873/13, 1 BvR 2618/13 Rn. 93.

Diese Verordnung würde im Schwerpunkt die Vertraulichkeit der Kommunikation (Fernmeldegeheimnis), die Verarbeitung von Kommunikationsdaten (bisher Verkehrsdaten) und das Speichern und Auslesen von Informationen auf Endeinrichtungen (Cookies) regeln.[11] Durch die unmittelbare Anwendbarkeit einer EU-Verordnung zu diesen Themen, würde die e-Privacy-Verordnung das deutsche TDDDG ablösen. Allerdings konnten sich die EU-Kommission, das Europäische Parlament und der Rat der Europäischen Union in den Trilog-Verhandlungen bisher nicht auf einen Gesetzesentwurf einigen. Nach der Europawahl Anfang Juni 2024 wird schon bald eine neue EU-Kommission die Arbeit aufnehmen. Die neue EU-Kommission könnte dann auch den bisherigen Vorschlag der e-Privacy-Verordnung zurücknehmen und einen neuen Versuch wagen.[12]

11 BfDI, https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telemedien/ePrivacy_Verordnung.html (zuletzt abgerufen am 10.7.2024).

12 Henning, https://netzpolitik.org/2024/fuer-die-naechste-eu-kommission-welche-digitalen-baustellen-bleiben-offen/ (zuletzt abgerufen am 10.7.2024).

DFN Infobrief-Recht-Aktuell

- ## Datenschutzrecht/Arbeitsrecht: Veröffentlichung eines Positionspapiers zum Beschäftigtendatenschutz durch den Hamburgischen Beauftragten für den Datenschutz und Informationsfreiheit (HmbBfDI) Thomas Fuchs

  Das am 6. Juni 2024 veröffentlichte Positionspapier „Bewerberschutz und Recruiting im Fokus“ beleuchtet die Entwicklungen im Bewerberdatenschutz unter Beachtung der Zunahme von KI-Tools einschließlich Lebenslaufparsern und Emotionsanalysen.

  Hier erhalten Sie den Link zum Positionspapier:

  https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240606_Information_Bewerberdatenschutz_und_Recruiting.pdf

- ## Arbeitsrecht: Entscheidung des LAG Düsseldorf vom 10. April 2024 – 12 Sa 1007/23 zur Durchführung einer Google-Recherche im Stellenbesetzungsverfahren

  Eine anlassbezogene Google-Recherche in einem Stellenbesetzungsverfahren ist gem. Art. 6 Abs. 1 S. 1 lit. b DSGVO zulässig. Es besteht jedoch eine Informationspflicht gem. Art. 14 DSGVO. Dabei kann ein Anspruch auf Schadensersatz geltend gemacht werden, wenn dieser nicht nachgekommen und die erlangten Informationen verwertet wurden.

  Hier erhalten Sie den Link zur Entscheidung:

  https://www.justiz.nrw.de/nrwe/arbgs/duesseldorf/lag_duesseldorf/j2024/NRWE_LAG_D_sseldorf_12_Sa_1007_23_Urteil_20240410.html

- ## Datenschutzrecht: EuGH entschied mit Urteil vom 20. Juni 2024 – C-590/22 erneut zum Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO

  Der EuGH bejahte einen Schadensersatzanspruch aufgrund der fehlerhaften Zusendung einer Steuererklärung. Es reiche die bloße Befürchtung aus, dass sensible Daten an Dritte gelangt sind. Jedoch müssten diese Befürchtung und die negativen Folgen tatsächlich vorliegen.

  Hier erhalten Sie den Link zur Entscheidung:

  https://curia.europa.eu/juris/document/document.jsf?text=&docid=287305&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=772905

- ## Europarecht: Urteil des EuGH zum Herkunftslandprinzip

  Der EuGH hat mit Urteil vom 30.Mai 2024 - C - 665/22 entschieden, dass Anbieter von Online-Vermittlungsdiensten nur den Regelungen ihres Herkunftsmitgliedstaats unterliegen.

  Hier erhalten Sie den Link zur Entscheidung:

  https://curia.europa.eu/juris/document/document.jsf?text=&docid=286563&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=3452870

Kurzbeitrag: The floor is yours, Bundesnetzagentur

Die Bundesnetzagentur ist nun zentrale Anlaufstelle für Aufsicht und Durchsetzung des neuen Rechtsrahmens für digitale Dienste

Von Nikolaus von Bernuth, Berlin

Der Digital Services Act (DSA) ist am 17. Februar 2024 vollumfänglich in Kraft getreten. Er ist ein zentraler Baustein der Digitalstrategie der EU und soll das Internet zu einem sicheren sowie grundrechts- und innovationsfreundlichen Raum machen. Wichtig wird eine effektive Aufsicht über die neuen Sorgfaltspflichten des DSA sein – in Deutschland wird dafür eine Koordinierungsstelle bei der Bundesnetzagentur geschaffen.

I. Die komplexe Aufsichtsarchitektur des DSA

Der DSA hat einen neuen Rechtsrahmen für Vermittlungsdienste (sprich: das Internet, wie wir es nutzen) geschaffen. Bis zuletzt war unklar, wer auf nationaler Ebene für Aufsicht und Durchsetzung des ambitionierten Pflichtenprogramms des DSA verantwortlich ist.[1] Seit das Digitale-Dienste-Gesetz (DDG) am 14. Mai 2024 in Kraft getreten ist, herrscht Klarheit. Ein Anlass, die neue Koordinierungsstelle für digitale Dienste und ihre Kompetenzen vorzustellen.

Die Aufsichtsstruktur des DSA ist komplex. Im Ausgangspunkt sind die Mitgliedsstaaten zuständig, Verstöße gegen den DSA zu ahnden. Zur Ausübung ihrer nationalen Aufsichtskompetenz betrauen sie ihre bestehenden oder neu eingerichteten Behörden mit dieser Aufgabe. Daneben ist aber auch die Europäische Kommission zuständig, insbesondere für die sehr großen Plattformen und Suchmaschinen.[2] Unter Umständen können sogar beide aktiv werden (vgl. Art. 56 ff. DSA). Außerdem soll ein europäisches Gremium unabhängigen Rat erteilen und im Streitfall vermitteln. Auch Zivilgesellschaft und Wissenschaft sollen Kontrollaufgaben übernehmen. Schließlich setzt der Gesetzgeber auf die private Rechtsdurchsetzung durch Nutzer:innen.

Um sicherzustellen, dass die Verantwortung im Mitgliedsstaat klar verteilt ist und es einen zentralen Ansprechpartner gibt, verpflichtet der DSA die Mitgliedsstaaten, einen Koordinator für digitale Dienste zu benennen (Art. 49 ff. DSA). In Deutschland ist dies eine neu eingerichtete Koordinierungsstelle in der Bundesnetzagentur (BNetzA) (§ 14 Abs. 1 DDG). Als zentrale deutsche Infrastrukturbehörde nimmt die BNetzA bislang Aufsichtsaufgaben in den Sektoren Energie, Telekommunikation, Post und Eisenbahnen wahr. Auch Verbraucherschutz gehört zum Aufgabenbereich. Dieses Profil sowie die vorhandene Kompetenz im Bereich digitaler Plattformen und die Erfahrung in der Zusammenarbeit mit anderen Behörden, auch innerhalb der EU, qualifizieren die BNetzA nach Ansicht des Gesetzgebers zur neuen Aufgabe.[3]

---

1 Zu den einzelnen Pflichten bereits Gielen, Digital Services Act: Das Plattformgrundgesetz?, DFN-Infobrief Recht 03/2021; John, Geschenke verpacken leicht gemacht: Transparenz ist in!, DFN-Infobrief Recht 12/2023; Rennert, Brüssel reguliert das schon, DFN-Infobrief Recht 06/2022.

2 Dies sind gem. Art. 30 DSA alle benannten Plattformen/Suchmaschinen mit über 45 Mio. mtl. aktiven Nutzer:innen.

3 Drucksache 20/10031, S.73f.

II. Die Koordinierungsstelle für digitale Dienste

Die frisch geschaffene Koordinierungsstelle wird mehrere Funktionen haben. Bei ihr soll erstens die deutschlandweite Aufsicht und Durchsetzung des DSA zusammenlaufen. Dazu gehört die behördliche Aufsicht, für die neben der BNetzA auch weitere Stellen zuständig sind, zum Beispiel die Bundesbeauftragte für Datenschutz und Informationssicherheit.[4] Zweitens ist sie Anlaufstelle für Nutzer:innen, die etwa geltend machen wollen, dass eine Plattform kein beziehungsweise ein unzureichendes Moderationssystem für rechtswidrige Inhalte bereithält. Drittens verleiht die Koordinierungsstelle qualifizierten zivilgesellschaftlichen Organisationen auf Antrag den Status als „Trusted Flagger“ (Art. 22 DSA). Sie können Inhalte auf digitalen Diensten melden; ihre Hinweise müssen Online-Plattformen priorisiert bearbeiten. Viertens lässt die Koordinierungsstelle die Stellen für außergerichtliche Streitbeilegung zu.

Digitale Dienste werden erklärtermaßen grenzübergreifend tätig. Aufsicht und Durchsetzung des DSA erfordern daher auch unionsweite Strukturen, die möglichst reibungslos ineinandergreifen. In der EU-weiten Zusammenarbeit ist die Koordinierungsstelle die deutsche Ansprechpartnerin. Sie entsendet eine Vertretung in das europäische Gremium für digitale Dienste und bespricht mit den Koordinatoren der anderen Mitgliedsstaaten etwaige Mängel in der Aufsicht. So könnte etwa die Koordinierungsstelle aktiv werden, wenn sie feststellt, dass ein anderer Mitgliedsstaat seine Aufsichtspflichten nicht erfüllt (Art. 58, 59 DSA).

Auch soweit es um den – für Hochschulen besonders interessanten – Datenzugang für zugelassene Forschende gem. Art. 40 Abs. 4 DSA[5] geht, ist die Koordinierungsstelle beteiligt: Sie überprüft Forschungsvorhaben auf ihre Zulässigkeit nach den Kriterien des DSA und erteilt dann den Status als zugelassener Forscher. Auf dieser Basis beantragt die Stelle bei den Plattformen Datenzugang für die Forschenden.

III. Ausblick

Die Koordinierungsstelle wirkt an nahezu jeder Schnittstelle des DSA mit – als zentraler Akteur in Fragen der behördlichen Aufsicht, aber auch in wichtiger Funktion bei den zivilgesellschaftlichen Instrumenten, die der DSA bereithält, um die großen Online-Plattformen aus diversen Perspektiven zu beaufsichtigen. Weil viele Akteure beteiligt sind und der DSA einen großen Strauß an Pflichten bereithält, ist es sinnvoll, die Kompetenz zu bündeln – solange die Koordinierungsstelle hinreichend ausgestattet ist.

Wichtig ist zudem: Die Koordinierungsstelle ist zwar im Haus der BNetzA angesiedelt, sie soll aber unabhängig agieren und keinen Weisungen unterliegen (§ 15 DDG).[6] Dies ist verfassungsrechtlich geboten; die Medienaufsicht ist nach deutschem, aber auch nach europäischem Recht staatsfern zu organisieren.[7] Die Politik muss daher darauf achten, dass die Koordinierungsstelle tatsächlich „staatsfern“ arbeiten kann und gerade das Bundeswirtschaftsministerium, dem die BNetzA direkt untersteht, keinen Einfluss ausübt. Hierzu könnte auch der Beirat (§ 21 DDG), der sich aus Wissenschaft, Zivilgesellschaft und Wirtschaftsverbänden zusammensetzt und dieser Tage nominiert wird, einen Beitrag leisten. [8]

Wer mit der Koordinierungsstelle in Kontakt treten möchte, findet auf https://www.dsc.bund.de die wesentlichen Informationen und Möglichkeiten, direkt auf digitalem Weg ein Anliegen vorzubringen.

---

4 Zur jüngsten Neubesetzung siehe Müller, Neue Wächterin der Daten, DFN-Infobrief 06/2024.

5 Näher hierzu Gielen, Digital Services Act: Das Plattformgrundgesetz?, DFN-Infobrief Recht 03/2021.

6 Umsetzung von Art. 50 Abs. 2 DSA; kritisch zur Ansiedlung an der Bundesnetzagentur vor dem Hintergrund des Gebots der Staatsferne Kreißig, AfP 2023, 389 (392).

7 Vgl. etwa Art. 30 der Richtlinie über audiovisuelle Mediendienste (RL (EU) 2018/1808); zur Staatsferne in der Rundfunkaufsicht BVerfG, Urt. v. 25. März 2014 – 1 BvF 1/11, 1 BvF 4/11.

8 Erste Berichte zum Personal: https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/dsc-beirat-die-ersten-vier-mitglieder-sind-bekannt (zuletzt abgerufen am 04.07.2024).

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