„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht

10 / 2025
Oktober 2025

Die Kommerzialisierung der Wissenschaft

Open Access-Zugriff auf Publikationen und Datentracking durch Wissenschaftsverlage bergen Chancen und Risiken

Von Anna Maria Yang-Jacobi, Berlin

Die Wissenschaft lebt bekanntlich vom Diskurs. Für den wissenschaftlichen Austausch ist es essenziell, Forschungsergebnisse zu veröffentlichen. Nur so können die gewonnenen Erkenntnisse diskutiert und weitergehend untersucht werden. Den Zugriff auf die Wissenschaftszeitschriften gewähren die Bibliotheken der Hochschulen und Forschungseinrichtungen. Das ist jedoch mit hohen Kosten verbunden. Dabei hat sich das Geschäftsmodell der Wissenschaftsverlage in den letzten Jahren verändert: Neben Open Access-Zugängen zu Publikationen spielt die Sammlung und Analyse von Daten mittlerweile eine große Rolle. Die Veränderungen haben weitreichende Folgen für die Wissenschaft und sollen im Folgenden vorgestellt werden.

I. Zugang zu wissenschaftlichen Publikationen

In Deutschland ist die Wissenschaftsfreiheit als Grundrecht nach Art. 5 Abs. 3 S. 1 Grundgesetz (GG) geschützt. Nach dem Hochschulurteil des Bundesverfassungsgerichts (BVerfG) von 1973 ist Wissenschaft „jede Tätigkeit, die nach Inhalt und Form als ernsthafter und planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist“.[1] Die Wissenschaft kann weiter aufgeteilt werden in Forschung und Lehre, die jeweils auch vom Grundrechtsschutz umfasst sind. Die Forschung ist die „geistige Tätigkeit mit dem Ziele, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen“.[2] Zum Schutzbereich der Wissenschaftsfreiheit gehört gerade auch die Verbreitung von Forschungsergebnissen.[3] Das Grundrecht gewährleistet dabei nicht nur einen Schutz vor staatlichen Eingriffen in die Wissenschaftsfreiheit. Vielmehr muss der Staat daneben auch grundsätzlich dafür sorgen, dass Bedingungen geschaffen werden,[4] unter denen sich die Wissenschaft frei entfalten kann. Staatliche wissenschaftliche Institutionen haben also für ihre wissenschaftliche Tätigkeit einen Anspruch auf Personal- und Sachmittel, finanzielle Mittel sowie darauf, an Kollektivgütern wie an Bibliotheksdiensten teilzuhaben.

Für Forschende ist die Veröffentlichung der Forschungsergebnisse von großer Bedeutung. Durch Veröffentlichungen in Fachpublikationen werden Wissenschaftler:innen inter- und intradisziplinär wahrgenommen und können sich ein gewisses Ansehen aufbauen. Dabei sind die erarbeiteten Werke nach § 2 Urheberrechtsgesetz (UrhG) geschützt. Die Autor:innen haben entsprechende Rechte aus dem Urheberrechtsgesetz, also allen voran die Urheberpersönlichkeitsrechte nach §§ 12 ff. UrhG, die Verwertungsrechte nach §§ 15 ff. UrhG und die Einräumung von Nutzungsrechten nach § 31 UrhG.

Die Veröffentlichung bzw. Verbreitung der Forschungsergebnisse erfolgt regelmäßig über private Wissenschaftsverlage, die eine Vielzahl an wissenschaftlichen Zeitschriften verantworten. In der Regel räumen die Verfasser:innen den Verlagen

1 BVerfG, Urt. vom 29.5.1973, NJW 1973, 1176 - Hochschulurteil.

2 BVerfG, Urt. vom 29.5.1973, NJW 1973, 1176 - Hochschulurteil.

3 BeckOK GG-Kempa/Rossa, GG Art. 5 Rn. 182.

4 Gärditz, Hochschulorganisation und verwaltungsrechtliche Systembildung, 2009, S. 274 ff.

bei Zeitschriftenbeiträgen ein ausschließliches Nutzungsrecht nach § 38 Abs. 1 S. 1 UrhG ein. Oftmals[5] erhalten sie jedoch kein Honorar für ihre Beiträge. Als private Unternehmen handeln die großen Wissenschaftsverlage dennoch gewinnorientiert und stellen die Beiträge nur gegen Entgelt zur Verfügung.

Diese Kommerzialisierung von wissenschaftlichen Erzeugnissen ist auf das Maxwell-Garfield-System[6] zurückzuführen. Nach dem Zweiten Weltkrieg sah der britische Verleger Robert Maxwell als einer der ersten das kommerzielle Potenzial der Wissenschaft. Speziell auf dem Markt der wissenschaftlichen Zeitschriften herrschte dauerhaft Nachfrage über Bibliotheken und Forschungseinrichtungen, die ihren Wissenschaftler:innen den Zugriff auf die aktuelle Literatur gewährleisten sollten. Gleichzeitig waren jene Wissenschaftler:innen auch bereit, die Inhalte ohne zusätzliche Vergütung zur Verfügung zu stellen. In der Folge gründeten die Wissenschaftsverlage immer mehr Zeitschriften, die wiederum von den Einrichtungen erworben wurden. Der Preis konnte konstant gesteigert werden, während die Kosten nicht signifikant wuchsen. Die Kosten hinter den Publikationen, also vor allem die Erarbeitung der Forschungsergebnisse selbst, lagen sowieso größtenteils aufseiten der Öffentlichkeit (sofern es Forschung an öffentlich finanzierten Einrichtungen betraf), während der Gewinn aufseiten der Verlage erfolgte. Mit der Masse an unterschiedlichen Zeitschriften fiel es den Bibliotheken zunehmend schwerer, zu beurteilen, welche tatsächlich gekauft werden sollten. Eugene Garfield entwickelte 1955 in den USA einen ersten Index, über den man die Zitierungen von Artikeln in anderen Beiträgen nachverfolgen konnte. Dieser wurde ein wichtiges Hilfsinstrument, um den sogenannten „Einflussfaktor" der Zeitschriften zu bestimmen. Der Einflussfaktor zeigt, wie oft ein Beitrag einer bestimmten Zeitschrift in anderen Beiträgen pro Jahr im Durchschnitt zitiert wurde. So konnten Bibliotheken besser beurteilen, welche Zeitschriften sie erwerben wollten. Die Grenzen von Wissenschaft und Wirtschaft vermischten sich beim Publizieren zunehmend.

II. Das „Geschäftsmodell" der Verlage im Wandel

Mit der Digitalisierung haben sich auch die Tätigkeiten der großen Wissenschaftsverlage verändert. Heutzutage gibt es neben physischen Werken vermehrt (rein) online zugängliche e-Publikationen und Literaturdatenbanken. So hat sich auch das Geschäftsmodell der Wissenschaftsverlage gewandelt.

1. Einnahmen über Subskriptionsmodell

In der Vergangenheit generierten Wissenschaftsverlage einen Großteil ihres Umsatzes über Abonnements. Die Bibliotheken der Hochschulen und Forschungseinrichtungen schlossen dafür Verträge mit den jeweiligen Verlagen, um ihren Angehörigen Zugriff auf Zeitschriften oder Sammelbände zu ermöglichen. Mitte der 1990er Jahre kam es jedoch zur „Zeitschriftenkrise". Die Preise der Zeitschriftenabonnements stiegen so stark an, dass die Bibliotheken mit ihrem begrenzten und oftmals stagnierenden Haushalt nicht mehr in der Lage waren, die Preise zu zahlen. Die Abonnements konnten nicht mehr fortgeführt werden. Daraus folgten jedoch noch höhere Preise. Schließlich mussten die Wissenschaftsverlage nun versuchen, die Einnahmeverluste auszugleichen. Die Leidtragenden waren die Wissenschaftler:innen – vor allem an Einrichtungen und in Ländern, die finanziell weniger gut aufgestellt waren. Ohne Subskriptionsmöglichkeit blieb ihnen der Zugang zu wichtigen Publikationen verwehrt. So kam es in der Wissenschaft zum Konsens, dass Alternativen zum Subskriptionsmodell notwendig waren bzw. dieses angepasst werden musste.

2. Einnahmen über Open Access-Veröffentlichungen

In den frühen 2000ern entwickelte sich ein neuer Ansatz: die Open Access-Veröffentlichung.[7] Open Access bedeutet, dass Publikationen für die wissenschaftliche Gemeinschaft und die Öffentlichkeit allgemein im Internet frei zugänglich sind. Damit

5 Die Rechtswissenschaften sind in dieser Hinsicht aber zum Beispiel eine Ausnahme, siehe Rux, ZUM 2023, 405, 407 f.

6 Siehe dazu Altschaffel et. al, RuZ 2024, 23, 23 ff. sowie ausführlich Neff, Issues in Science and Technology, 2020, https://issues.org/how-academic-science-gave-its-soul-to-the-publishing-industry/ (alle Links dieses Beitrags wurden zuletzt am 3.9.2025 abgerufen).

7 Entscheidend waren die Budapest Open Access Initiative (BOAI), das Bethesda Statement on Open Access Publishing sowie die Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities.

soll wissenschaftliche Literatur kostenlos und ohne technische und rechtliche Barrieren vielseitig genutzt werden können. In den letzten 20 Jahren hat sich dabei einiges getan. Zahlreiche Open Access-Projekte und Initiativen[8] starteten auf internationaler, europäischer und nationaler Ebene. Auch die Bundesländer wurden aktiv.[9] So hat jedes Bundesland eine Open Access-Strategie.[10] Zudem wurden bereits 2023 gemeinsame Leitlinien von Bund und Ländern entwickelt.[11]

Dabei existieren verschiedene Open Access-Modelle. Die bekanntesten sind dabei „Gold Open Access" und „Green Open Access". Als „Gold Open Access" ist die für die Leserschaft frei zugängliche Erstveröffentlichung in reinen Open Access-Zeitschriften/Formaten bekannt. Die Finanzierung der Beiträge erfolgt manchmal über die Einnahmen von Subskriptionen der anderen Zeitschriften des Verlags. Häufiger handelt es sich jedoch um eine bloße „Verlagerung" der Kosten: Anstelle der Leserschaft zahlen nun die Verfasser:innen sogenannte Article Processing Charges (APCs) pro veröffentlichtem Artikel für den freien Zugang der Lesenden. „Green Open Access" beschreibt die frei zugängliche Zweitveröffentlichung von Beiträgen aus zugangsbeschränkten Zeitschriften. Die Zweitveröffentlichung kann zeitgleich oder nachträglich zur Erstveröffentlichung erfolgen und ist oft erst nach einer gewissen Frist möglich. Zusätzlich gibt es auch das „Hybrid Open Access". Dies betrifft Beiträge in Zeitschriften, die vom Verlag über ein Abonnement angeboten werden. Die Autor:innen können ihre Artikel aber über die Zahlung von APCs „freikaufen" und so nur den entsprechenden Artikel frei zugänglich machen.

Bisher bedeutet die Umstellung auf Open Access also nicht, dass die großen Wissenschaftsverlage nun massive Einnahmeeinbußen verzeichnen mussten. Der wissenschaftliche Gedanke von „publish or perish", also „wer veröffentlicht, der bleibt", besteht weiterhin. Auch heutzutage stehen Wissenschaftler:innen unter einem enormen Publikationsdruck. Die Veröffentlichungen sollen dabei gerade in möglichst namhaften Zeitschriften und Verlagen erfolgen. Entsprechend verzeichnen die großen Wissenschaftsverlage weiterhin hohe Gewinne – anstelle der Subskriptionsgebühren steigen jetzt die Ausgaben für APCs nach Schätzungen stetig an.[12] Bei öffentlich finanzierter Forschung zahlt der Staat also weiterhin für die Forschung selbst und auch für ihren späteren Abruf.[13]

3. Einnahmen aus Datentracking?

Zusätzlich haben Wissenschaftsverlage ihr Geschäftsmodell um eine neue Tätigkeit erweitert: das Datentracking. Viele Verlage bieten mittlerweile Informationsdienste wie Literaturdatenbanken an. Über die digitale Verfügbarkeit der Beiträge und die Nutzung der digitalen Informationsdienste können die Verlage Echtzeitdaten über die Interessen und das Verhalten von Hochschulen, Forschungseinrichtungen und den Forschenden tracken, also festhalten und speichern, sowie analysieren und weiterverwerten. Bei den Daten handelt es sich um Zugriffs- und Nutzungsdaten oder Daten zur Verweildauer bei bestimmten Beiträgen. Zudem können so individuelle Profile der Wissenschaftler:innen angelegt werden. Der Ausschuss für Wissenschaftliche Bibliotheken und Informationssysteme (AWBI) hat die möglichen Verfahren zur Datengewinnung 2021 zusammengefasst.[14]

Das Festhalten und Speichern der Daten der Wissenschaftler:innen verstärkt die Macht der Verlage weiter. Sofern die Datenbanken

8 Für genauere Informationen siehe https://open-access.network/informieren/open-access-grundlagen/geschichte-des-open-access.

9 Zuletzt zum Beispiel in Mecklenburg-Vorpommern, https://www.heise.de/news/Freier-Zugang-zu-Forschung-Mecklenburg-Vorpommern-investiert-in-Open-Access-10512085.html.

10 https://open-access.network/services/oaatlas/laenderdossiers.

11 BMBF, Open Access in Deutschland, Mai 2023, https://www.bmftr.bund.de/SharedDocs/Publikationen/DE/1/772960_Open_Access_in_Deutschland.pdf?__blob=publicationFile&v=5.

12 Haustein et al., Estimating global article processing charges being paid to six publishers for open access between 2019 and 2023, 23.07.2024, https://arxiv.org/pdf/2407.16551.

13 Blankertz, Warum Gewinne von Wissenschaftsverlagen die Gesellschaft doppelt kosten, 03.12.2023, https://netzpolitik.org/2023/oeffentliches-geld-oeffentliches-gut-warum-gewinne-von-wissenschaftsverlagen-die-gesellschaft-doppelt-kosten/.

14 Ausführlich zu den Methoden siehe AWBI (2021): Datentracking in der Wissenschaft: Aggregation und Verwendung bzw. Verkauf von Nutzungsdaten durch Wissenschaftsverlage, 28.10.2021, S. 9 f., https://www.dfg.de/resource/blob/174922/5b903b1d487991f2d978e3a308794b4c/datentracking-papier-de-data.pdf.

und die weiteren Informationsdienste jedoch über die Webseiten der Hochschulen angeboten werden, besteht ein weiteres Problem. Gerade öffentliche Hochschulen und Bibliotheken haben den Auftrag, den Schutz der Privatsphäre von Nutzenden zu gewährleisten. Durch das Datentracking besteht die Gefahr eines Eingriffs in Grundrechte, allen voran das europarechtlich gewährleistete Recht am Schutz der eigenen Daten nach Art. 8 der Charta der Grundrechte der EU (GRCh) und die Wissenschaftsfreiheit nach Art. 5 Abs. 3 GG, Art. 13 GRCh.

Nichtsdestotrotz ist es wichtig zu betonen, dass unklar ist, welche Art der Datengewinnung von den Wissenschaftsverlagen tatsächlich ausgeübt wird. Eine weitreichende Verwendung der Daten kann aber nicht ausgeschlossen werden.[15] Außerdem darf nicht vergessen werden, dass Datenanalysen auch positives Potenzial bergen. Für Bibliotheken ist es beispielsweise hilfreich, über Datenanalysen einen Einblick in den gesamten Forschungszyklus zu bekommen.

III. Umgang mit der Macht der Wissenschaftsverlage?

Die großen Wissenschaftsverlage wachsen immer weiter. Der deutsche Wissenschaftsverlag Springer Nature machte 2024 beispielsweise insgesamt einen Gewinn von 512 Millionen Euro. Gerade das Geschäft mit Open Access-Zeitschriften war entscheidend für das Wachstum.[16] Das Interesse an den Publikationen besteht also unverändert, und Hochschulen und Forschungseinrichtungen sind weiterhin auf den Erwerb der Zeitschriften angewiesen. Es gibt allerdings verschiedene Ansatzpunkte, um die Vertragsmodalitäten zu verändern.

1. Der DEAL

Bereits 2014 bildet sich über die Allianz der Wissenschaftsorganisationen das sogenannte DEAL-Konsortium unter Leitung der Hochschulrektorenkonferenz. Anstatt individuell und hinter geschlossenen Türen mit den Wissenschaftsverlagen zu verhandeln, wollte man als Gemeinschaft für bessere und bundesweit geltende Vertragskonditionen mit besonderem Fokus auf Open Access-Veröffentlichungen einstehen. So sollten die Nutzungsrechte und Kosten über die Konsortialverträge der „DEAL"-Initiative angemessener gestaltet werden. Die Vertragspartner sind die aus Veröffentlichungsperspektive größten Wissenschaftsverlage in Deutschland: Elsevier, Springer Nature und Wiley. An den geschlossenen DEAL-Verträgen können bei Bedarf alle deutschen wissenschaftlichen Einrichtungen und auch andere Einrichtungen wie Behörden oder private Hochschulen teilnehmen. Die genauen Voraussetzungen stehen in den jeweiligen Verträgen. Diese sind transparent einsehbar und enthalten standortunabhängige Konditionen. Durch den Abschluss der Verträge gewähren die Verlage den teilnehmenden Institutionen einen Volltextzugriff auf elektronische Zeitschriften und die Möglichkeit von Open Access-Publikation ohne Zusatzkosten. Für die Verlage liegt der Anreiz der DEAL-Verträge darin, dass Wissenschaftler:innen voraussichtlich bevorzugt in Zeitschriften veröffentlichen werden, in denen sie wegen des DEAL-Vertrags nicht zahlen müssen. Die erste Vertragsphase verlief von 2019 bis 2023.

Bereits 2017 kritisierten konkurrierende Verlage den „DEAL".[17] Kleinere Verlage würden benachteiligt. Diese kleineren Verlage seien es aber vor allem, die nicht gewinnorientiert arbeiteten, ihre Kosten offenlegten und zur Vielfalt der Publikationsmöglichkeiten beitrügen. Beschwerden an das Bundeskartellamt wegen eines vermeintlichen kartellrechtlichen Marktmachtmissbrauchs des „DEAL" blieben aber erfolglos.

Nach Auslauf der ersten Vertragslaufzeiten verhandelte das Konsortium erneut mit denselben drei Wissenschaftsverlagen für den Zeitraum 2024 bis 2028. Wie bereits in der ersten Vertragsphase steht in allen drei Verträgen,[18] dass Open Access-Publikationen in den Zeitschriften für die teilnehmenden Einrichtungen möglich sein sollen. Die teilnehmenden Einrichtungen erhalten in der Regel einen Rabatt von 15-20 % auf die APCs und einen Lesezugriff auf die Zeitschrifteninhalte der Verlage. Das genaue

15 Kunz, RuZ 2022, 77, 87.

16 https://group.springernature.com/de/group/media/press-releases/ergebnisse-geschaeftsjahr-2024/27762604.

17 https://www.boersenverein.de/politik-positionen/projekt-deal/.

18 Die Verträge sind alle online abrufbar. Der Vertrag mit Elsevier, https://pure.mpg.de/rest/items/item_3523659_2/component/file_3527946/content; Vertrag mit Springer Nature, https://pure.mpg.de/rest/items/item_3551270_4/component/file_3580149/content; Vertrag mit Wiley, https://pure.mpg.de/rest/items/item_3551268_2/component/file_3551953/content.

Preismodell unterscheidet sich je nach Vertrag etwas. Allen gemein ist jedoch eine festgelegte Publish and Read (PAR) Gebühr als einheitlicher Pauschalbetrag der Teilnehmenden. Die PAR-Gebühr wird für jeden Beitrag fällig, den die Verfasser:innen in den Zeitschriften der Verlage veröffentlichen möchten. Sie ersetzt die zusätzlichen Kosten für Wissenschaftler:innen beim Hybrid Open Access-Modell und die Subskriptionsgebühren für einen umfassenden Lesezugang. Die Veröffentlichung eines Beitrags kostet je nach Zeitschrift 2.500 Euro bis 6.450 Euro. Allerdings sind in allen Verträgen ab 2025 jährliche Preissteigerungen der PAR-Gebühr von 3 bis 4 Prozent festgelegt.

Im Rahmen der zweiten Vertragsverhandlungen wurde erstmals auch das Datentracking der Verlage thematisiert.[19] Aufseiten der Forschung war man der Ansicht, dass die Datenverarbeitung durch die Verlage eine gemeinsame Datenverarbeitung im Sinne des Art. 26 Datenschutzgrundverordnung (DSGVO) sei.[20] Das würde bedeuten, dass die Wissenschaftsorganisationen und die Verlage gemeinsam über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten entscheiden. Allerdings waren die Verlage der Ansicht, dass die Verarbeitungsschritte klar abgrenzbar seien, und lehnten eine gemeinsame Verantwortung ab.[21] Zugestanden wurde nur, dass bei Verletzungen des Datenschutzes und des Persönlichkeitsrechts im Innenverhältnis die Verantwortung zu übernehmen sei, um die Bibliotheken so von möglichen finanziellen Forderungen freizustellen. Auch die Datenübertragung ins Ausland wurde diskutiert. Im Ergebnis gehen die Vertragsregelungen aber nicht über die gesetzlichen Vorgaben hinaus. Regelungen zum Training von KI-Anwendungen[22] wurden nicht getroffen.

2. Öffentliche Forschungsförderung als Modell der Zukunft

Der DEAL könnte jedoch auch nur eine Übergangslösung sein. Alternativ könnte die Wissenschaft gemeinsam mit Bibliotheken und wissenschaftsorientierten, nicht kommerziellen Verlagen die Nutzung wissenschaftlicher Erkenntnisse organisieren. Die Nationale Akademie der Wissenschaften Leopoldina schlug 2025 in einem Diskussionspapier[23] ein neues Konzept vor. Nach diesem Konzept sollen wissenschaftliche Publikationen genau wie öffentliche Forschung selbst durch öffentliche Mittel finanziert werden. Das wird teilweise bereits versucht. Um mit den bisherigen Standards der Publikationen mithalten zu können, muss es aber auch eine dauerhafte Qualitätskontrolle geben. Bereits jetzt gibt es schon anerkannte Zeitschriften von Fachgesellschaften. Gerade diese Fachgesellschaften oder auch Akademien sollen Anträge zur direkten und dauerhaften Finanzierung von Zeitschriften stellen können. Die Anträge sollen dabei ähnlich wie Forschungsanträge begutachtet werden, um eine Qualitätskontrolle zu gewährleisten. Sofern eine Zeitschrift eine langfristige Finanzierung erhält, folgen regelmäßige Re-Evaluationen. Für den technischen Betrieb kann über Ausschreibungen auf die Expertise der kommerziellen Verlage zurückgegriffen werden. Zuletzt soll nach diesem Finanzierungsmodell die dauerhafte Archivierung separat durch die Bibliotheken selbst erfolgen.

3. Verschiedene Maßnahmen gegen die Praxis der Wissenschaftsverlage

Im Urheberrecht führte der deutsche Gesetzgeber 2014 einen zusätzlichen Absatz ein, der die Open Access-Veröffentlichung von Zeitschriftenartikeln betrifft. § 38 Abs. 4 UrhG besagt, dass ein Beitrag, der im Rahmen einer mehrheitlich mit öffentlichen Mitteln finanzierten Forschungstätigkeit entstanden ist und in einer mindestens halbjährlich erscheinenden Zeitschrift veröffentlicht wurde, 12 Monate nach der Erstveröffentlichung zu nicht gewerblichen Zwecken Open Access veröffentlicht werden kann, obwohl dem Verlag oder Herausgeber ein ausschließliches Nutzungsrecht eingeräumt wurde. Dies umfasst also das „Green Open Access“. Die Verfasser:innen haben damit unter den genannten Voraussetzungen eine gesetzlich garantierte Möglichkeit zur Zweitveröffentlichung.

Über das Kartellrecht versuchten mehrere Konkurrenten bereits, gegen die Machtstellung der großen Wissenschaftsverlage

19 Ausführlich siehe Interview des Laborjournal mit dem Mitglied der DEAL-Gruppe, Bernhard Mittermaier, 30.9.2024, https://www.laborjournal.de/editorials/m_3095.php?consent=1 sowie Altschaffel et al., RuZ 2024, 23, 27 ff.

20 Zur gemeinsamen Verantwortung siehe Geiselmann, Gemeinsam sind wir verantwortlich, DFN-Infobrief Recht 1/2024.

21 Altschaffel et al., RuZ 2024, 23, 31.

22 Zum Urheberrecht und KI-Training, Müller, Die Menge macht‘s, DFN-Infobrief Recht 11/2024.

23 Tautz et al., 2025, Diskussionen Nr. 38, https://www.leopoldina.org/fileadmin/redaktion/Publikationen/Nationale_Empfehlungen/2025_Leo_Diskussionspapier_zur_Finanzierung_DE.pdf.

vorzugehen. Das Bundeskartellamt und auch die EU-Kommission[24] sahen wegen des Verhaltens und der Marktstellung der Wissenschaftsverlage jedoch keinen Bedarf, kartellrechtlich tätig zu werden. Gerade bezogen auf die Datenanalysetätigkeiten weisen die Verlage jedoch Parallelen zu Online-Plattformen auf. Mit dem Digital Markets Act (DMA)[25] existieren zwar spezielle Regelungen zur Marktmacht von großen Plattformen in der Digitalwirtschaft. Allerdings sind die Voraussetzungen zur Anwendbarkeit (Einstufung als Torwächter, engl.: Gatekeeper) nach Art. 3 DMA sehr eng und liegen bei den Wissenschaftsverlagen in der Regel nicht vor.[26]

Das Datentracking könnte gegen datenschutzrechtliche Regelungen verstoßen. Zu einer genauen Beurteilung sind jedoch ausführlichere Informationen zur Datenverarbeitung und zum technischen Hintergrund erforderlich. Die Wissenschaftler:innen könnten dafür zum Beispiel von ihrem Auskunftsrecht nach Art. 15 DSGVO Gebrauch machen. Für eine rechtmäßige Verarbeitung von personenbezogenen Daten muss eine der Bedingungen des Art. 6 Abs. 1 lit. a bis lit. f DSGVO erfüllt sein. Sofern die Datenverarbeitung nicht nach Art. 6 Abs. 1 lit. b-lit. f DSGVO erforderlich ist, bedarf es somit einer Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO. Gerade bezogen auf Webseiten sind für nicht erforderliche Tracking-Aktivitäten somit in der Regel auch Cookie-Banner zu setzen (§ 25 Abs. 1 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)), über die eine Einwilligung erfolgen kann. Neben den Wissenschaftsverlagen müssen auch die Wissenschaftseinrichtungen die Vorgaben der DSGVO einhalten. Ansonsten drohen Bußgelder (nur für nicht öffentliche Stellen) oder Schadensersatzansprüche (sowohl gegen öffentliche als auch nicht öffentliche Stellen). Nach Entscheidungen des Europäischen Gerichtshof (EuGH) liegt eine gemeinsame Verantwortlichkeit im Sinn des Art. 26 DSGVO vor, wenn über die Einbindung von (Dritt-)Diensten auf einer Webseite eine weitere Datenverarbeitung möglich gemacht wird.[27] So könnte es vergleichbar sein, wenn eine Wissenschaftseinrichtung die Datenverarbeitung durch einen Verlag ermöglicht oder selbst von der Datenverarbeitung profitiert. Aufgrund dessen schlugen die Vertreter:innen auf Seite der Wissenschaftsorganisationen während der zweiten DEAL-Verhandlungen eine Musterklausel zur gemeinsamen Verantwortlichkeit vor. Zusätzlich wollten sie die Verlage dazu verpflichten, eine jährliche Datenschutz-Folgenabschätzung durchzuführen, um mögliche Risiken besser einschätzen zu können. Weder die Musterklausel zur gemeinsamen Verantwortlichkeit noch die verpflichtende Datenschutz-Folgenabschätzung wurden Teil der zweiten DEAL-Verträge.[28] Gerade wegen des Datentrackings und den damit verbundenen Risiken einer unrechtmäßigen Verarbeitung oder Übermittlung personenbezogener Daten von Wissenschaftler:innen hat die Gesellschaft für Freiheitsrecht (GFF) gemeinsam mit einem Professor der Universität Regensburg im August 2024 eine Beschwerde gegen Springer Nature, Wiley und Nomos beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) eingereicht.[29] Es bleibt abzuwarten, wie die Datenschutzbehörde die Datenanalysetätigkeiten der Wissenschaftsverlage bewertet.

IV. Fazit und Ausblick

Im Bereich der Wissenschaftspublikationen befindet sich viel im Wandel. Es bleibt die Hoffnung, dass die zahlreichen Initiativen und Projekte zu Open Access bald Wirkung zeigen und der freie Zugang zu Wissenschaftspublikationen nach den mehr als 30-jährigen Bemühungen endlich zur allgemeinen Realität wird. Außerdem ist gerade das Tracking von personenbezogenen Daten der Wissenschaftler:innen durch die Verlage genau zu beobachten. Die Prüfung und Bewertung des Sachverhalts durch den LfDI BW könnte Klarheit schaffen. Als Datenschutzbehörde erhält dieser durch seine Kontrollen weitere Informationen zum technischen Hintergrund des Trackings und kann den Sachverhalt unabhängig bewerten. Langfristig gilt trotzdem, dass im Idealfall auf eine öffentliche Förderung der Wissenschaftspublikationen hingearbeitet werden sollte.

---

24 Die Beschwerde richtete sich gegen die RELX Group, dem Mutterkonzern von Elsevier, siehe Beschwerde vom 26.10.2018 und Antwort der EU-Kommission, https://zenodo.org/records/2565052#.YsbGUC-21-U.

25 Genauer zum DMA, siehe Rennert, Brüssel reguliert das schon, DFN-Infobrief Recht 6/2022.

26 So auch Kunz, RuZ 2022, 77, 90.

27 Nur beispielhaft EuGH, Urt. v. 29.7.2019, Rs. C-40/17 – Fashion ID, Rn. 80.

28 Siehe ausführlich Altschaffel et al., RuZ 2024, 23, 29 ff.

29 https://freiheitsrechte.org/themen/demokratie/wissenschaftstracking.

Das Recht auf Erklärung von KI-Entscheidungen – Teil 1

Sowohl die DSGVO als auch die KI-VO kennen ein Recht auf Erklärung – aber was bedeutet das eigentlich?

Von Philipp Schöbel, Berlin

In vielen Lebensbereichen werden Entscheidungen mithilfe von KI-Systemen gefällt. Menschen, die mit dem Ergebnis einer Entscheidung, zum Beispiel in Form einer Immatrikulation, Kreditvergabe oder Zusage eines Arbeitsverhältnisses, nicht einverstanden sind, stehen vor der Herausforderung, die Fehler der KI benennen zu müssen, wenn sie das Ergebnis rechtlich angreifen wollen. Zudem ist es im Interesse der Betroffenen zu erfahren, warum eine Entscheidung zu ihren Ungunsten ausgefallen ist. Die Verordnung über künstliche Intelligenz (KI-VO) regelt das sogenannte Recht auf Erläuterung ausdrücklich in Art. 86 KI-VO.[1] Lange Zeit war umstritten, ob auch die Datenschutz-Grundverordnung (DSGVO) ein sogenanntes Recht auf Erklärung enthält. Der Europäische Gerichtshof (EuGH) hat dies Anfang 2025 bejaht.[2]

I. KI-Einsatz an Hochschulen

Der Einsatz von KI in Forschung, Lehre und Hochschulverwaltung kann potenziell grundrechtssensible Bereiche berühren. So vielfältig wie die Einsatzmöglichkeiten von KI sind, so unterschiedlich können Grundrechtseingriffe und -verletzungen sein. Die Erstellung von Lehrinhalten mittels KI birgt andere Gefahren als etwa eine KI-gestützte Plagiatssoftware oder der Einsatz von KI innerhalb der Verwaltung. Neben den betroffenen Grundrechten der Angestellten (etwa dem Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit (i. V. m.) Art. 1 Abs. 1 Grundgesetz (GG) und Datenschutz nach Art. 7, 8 GRC) sind gerade auch die Grundrechte der Studierenden der Hochschulen zu beachten (zusätzlich etwa die Berufsfreiheit nach Art. 12 Abs. 1 S. 1 GG und Recht auf Bildung nach Art. 14 Abs. 1 Charta der Grundrechte der Europäischen Union (GRC)).

Insbesondere die Korrektur von Prüfungsleistungen mithilfe von KI kann für die betroffene Person weitreichende Folgen haben. Prüfungsrechtlich soll der Einsatz von KI nur zur Unterstützung bei der Entscheidungsfindung zulässig sein.[3] Die vollständige Übernahme der Prüfung ist dagegen unzulässig, weil die Prüfungsbewertung das Ergebnis einer menschlichen Entscheidung darstellen muss.[4] Unabhängig von der prüfungsrechtlichen Zulässigkeit des KI-Einsatzes besteht jedoch auch das Recht auf Erklärung, allerdings grundsätzlich unabhängig von der prüfungsrechtlichen Zulässigkeit des KI-Einsatzes. Dieses Recht kann aber auch vor der Anfechtung von Prüfungsentscheidungen

1 Die englische Sprachfassung spricht von „Right to explanation".

2 EuGH, Urteil v. 27.02.2025, C 203/22, ECLI:EU:C:2025:117 – Dun & Bradstreet Austria, abrufbar unter: https://curia.europa.eu/juris/document/document.jsf?text=&docid=295841&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=16295599; das Urteil wird in einem kommenden Beitrag ausführlich dargestellt (alle Links des Beitrags zuletzt abgerufen am 30.09.2025).

3 Schwartmann/Kurth/Köhler, Der Einsatz von KI an Hochschulen – eine rechtliche Betrachtung, OdW 2024, 161, 166, abrufbar unter: https://ordnungderwissenschaft.de/wp-content/uploads/2024/06/Gesamtausgabe.pdf.

4 Schwartmann/Kurth/Köhler, Der Einsatz von KI an Hochschulen – eine rechtliche Betrachtung, OdW 2024, 161, 166.

geltend gemacht werden, um den Sachverhalt für die Betroffenen aufzuklären.

Das europäische Sekundärrecht kennt verschiedene Erklärungsrechte. Für den Einsatz von KI-Systemen im Hochschulsektor sind dabei vornehmlich die Regelung des Art. 86 KI-VO und die Art. 13-15 DSGVO relevant.

II. Das Recht auf Erklärung in der DSGVO

Die DSGVO enthält mehrere einschlägige Vorschriften: Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g und Art. 15 Abs. 1 lit. h DSGVO sehen jeweils in Verbindung mit (i. V. m.) Art. 22 DSGVO Informationspflichten im Zusammenhang mit automatisierten Entscheidungen vor. Nach Art. 15 Abs. 1 lit. h DSGVO i. V. m. Art. 22 DSGVO hat die betroffene Person ein Recht auf Auskunft über ihre personenbezogenen Daten. Dieses Recht umfasst auch Informationen über das Bestehen einer automatisierten Entscheidungsfindung nach Art. 22 DSGVO und aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person. Art. 22 Abs. 1 DSGVO bezieht sich auf Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhen. Zudem muss die Entscheidung der betroffenen Person gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen. Die Voraussetzungen eines solchen Anspruchs werden im Folgenden dargestellt.

1. Anspruchsgegner

Zur Erklärung verpflichtet ist, wer Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist. Danach ist Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind mehrere Personen gemeinsame Verantwortliche im Sinne des Art. 26 Abs. 1 S. 1 DSGVO, kann der Betroffene das Recht auf Erklärung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen (vgl. Art. 26 Abs. 3 DSGVO).

2. Automatisierte Verarbeitung

Der Begriff der Verarbeitung wird in der DSGVO legaldefiniert (Art. 4 Nr. 2 DSGVO). Die Definition umfasst jeden Vorgang des Umgangs mit personenbezogenen Daten – von der Erhebung bis zur Löschung.[5] Eine Verarbeitung ist automatisiert, wenn sie durch Informationstechnik unterstützt wird und nicht vollständig manuell erfolgt.[6] Automatisiert umfasst auch die Verarbeitung mittels technisierter/computerisierter Datenverarbeitungsanlagen.[7]

3. Profiling

Profiling ist ein Unterfall der Verarbeitung. Die DSGVO definiert Profiling in Art. 4 Nr. 4 als „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“. Der Begriff umfasst die Erstellung, Aktualisierung und Verwendung von Profilen natürlicher Personen.[8] Ein klassisches Beispiel für Profiling ist die sogenannte Rasterfahndung.[9] Ein weiterer Fall von Profiling stellt die Verwendung von Analysetechniken (z. B. Datentracking) von Online-Anbietern dar.[10]

---

5 Gola, in: Gola/Heckmann, 3. Aufl. 2022, DS-GVO Art. 4 Rn. 35.

6 Roßnagel, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2. Aufl. 2025, DSGVO Art. 2 Rn. 14.

7 Spindler/Dalby, in: Spindler/Schuster, 4. Aufl. 2019, DS-GVO Art. 4 Rn. 10.

8 Ernst, in: Paal/Pauly, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 36.

9 Gola, in: Gola/Heckmann, 3. Aufl. 2022, DS-GVO Art. 4 Rn. 42.

10 Ernst, in: Paal/Pauly, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 39.

4. Ausschließlich auf die automatische Verarbeitung gestützt

Es ist außerdem erforderlich, dass die Entscheidung ausschließlich auf die automatisierte Verarbeitung gestützt wird.[11] Davon ist auszugehen, wenn keine inhaltliche Überprüfung durch eine natürliche Person stattgefunden hat.[12] Umfasst sind deshalb auch Fälle, in denen „ein Mensch – ohne eigene Erwägungen anzustellen – die automatisierte Vorgabe lediglich bestätigt oder übernimmt." [13]Im Gegensatz dazu liegt eine bloße automatisierte Vorbereitung einer Entscheidung vor, wenn ein Mensch, die automatisierte Entscheidung überprüft und als eigene Entscheidung umsetzt.[14] An die Überprüfung durch einen Menschen werden mehrere Anforderungen gestellt. Der überprüfende Mensch muss über die nötige Datengrundlage, die fachliche Qualifikation und technische Kompetenz sowie einen Entscheidungsspielraum verfügen.[15] Der EuGH hat entschieden, dass eine Entscheidung im Einzelfall auch dann vorliegt, „wenn ein auf personenbezogene Daten zu einer Person gestützter Wahrscheinlichkeitswert in Bezug auf deren Fähigkeit zur Erfüllung künftiger Zahlungsverpflichtungen durch eine Wirtschaftsauskunftei automatisiert erstellt wird, sofern von diesem Wahrscheinlichkeitswert maßgeblich abhängt, ob ein Dritter, dem dieser Wahrscheinlichkeitswert übermittelt wird, ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet."[16]

5. Involvierte Logik, Tragweite und Auswirkungen der Verarbeitung

Der Anspruch umfasst aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen. Teilweise wird angeführt, dass schon die tatsächliche Erklärbarkeit von Algorithmen an Grenzen stößt.[17] Darüber hinaus ist die Auslegung der Norm – also der Anspruchsinhalt – vielfach diskutiert worden. Problematisiert wurde etwa, wann eine Information „aussagekräftig" ist und welche Informationen von der „involvierten Logik" umfasst sind.[18] Das oben erwähnte Urteil des EuGH[19] befasst sich mit dem Anspruchsumfang und wird in einer kommenden Ausgabe des Infobriefs hinsichtlich dieser Punkte ausführlich dargestellt.

6. Anspruchsinhaber

Das Recht steht der betroffenen Person zu. Die Betroffenheit richtet sich nach Art. 4 Nr. 1 DSGVO.[20] Maßgeblich ist also, auf wen sich die Information bezieht. Die Rechte aus Art. 15 DSGVO sind nicht abtretbar oder vererbbar.[21] Allerdings kann ein Bevollmächtigter sowohl den Antrag nach Art. 15 Abs. 1 DSGVO stellen als auch die Information entgegennehmen.[22] Anspruchsinhaber:in bei dem Einsatz einer KI-gestützten Plagiatssoftware wäre etwa die Person, die die Arbeit ausgefertigt hat. Problematisch könnten Fälle sein, in denen eine dritte Person (unzulässigerweise) im Namen einer anderen etwa eine Hausarbeit verfasst. Hier ist es

11 Scholz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2. Aufl. 2025, DSGVO Art. 22 Rn. 29.

12 Scholz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2. Aufl. 2025, DSGVO Art. 22 Rn. 29 mwE.

13 Scholz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2. Aufl. 2025, DSGVO Art. 22 Rn. 29 mwE.

14 Scholz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2. Aufl. 2025, DSGVO Art. 22 Rn. 31; von Lewinski, in: BeckOK DatenschutzR, 52. Ed. 1.5.2025, DS-GVO Art. 22 Rn. 23.

15 Scholz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2. Aufl. 2025, DSGVO Art. 22 Rn. 30.

16 EuGH, Urteil v. 07.12.2023, C 634/21, ECLI:EU:C:2023:957 – OQ/Land Hessen, Rn. 75, abrufbar unter: https://curia.europa.eu/juris/document/document.jsf?text=&docid=280426&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=6554630; zur Vorlage an den EuGH durch das VG Wiesbaden siehe Tech, Scoring – bald nur noch als Entscheidung auf dem Platz?, DFN-Infobrief Recht 6/2023, S. 5.

17 Paal/Hennemann, in: Paal/Pauly, 3. Aufl. 2021, DS-GVO Art. 13 Rn. 31e.

18 Schmidt-Wudy, in: BeckOK DatenschutzR, 52. Ed. 1.5.2025, DS-GVO Art. 15 Rn. 78 mwE.

19 Siehe Fn. 2.

20 Dix, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2. Aufl. 2025, DSGVO Art. 15 Rn. 9.

21 Schmidt-Wudy, in: BeckOK DatenschutzR, 52. Ed. 1.5.2025, DS-GVO Art. 15 Rn. 35 mwE.

22 Franck, in: Gola/Heckmann, 3. Aufl. 2022, DS-GVO Art. 15 Rn. 28; Schmidt-Wudy, in: BeckOK DatenschutzR, 52. Ed. 1.5.2025, DS-GVO Art. 15 Rn. 35.

denkbar, dass beide Personen einen Anspruch aus Art. 15 Abs. 1 lit. h DSGVO i. V. m. Art. 22 DSGVO haben.

III. Das Recht auf Erklärung in der KI-VO

Art. 86 Abs. 1 KI-VO gewährt unter bestimmten Voraussetzungen ein Recht auf Erläuterung. Die Person muss zunächst von einer Entscheidung betroffen sein. Diese Entscheidung muss ein Betreiber auf der Grundlage der Ausgaben eines in Anhang III KI-VO[23] aufgeführten Hochrisiko-KI-Systems getroffen haben. Die Entscheidung muss zudem rechtliche Auswirkungen haben oder die Person in ähnlicher Art erheblich beeinträchtigen. Die Beeinträchtigung muss nach Ansicht der Person ihre Gesundheit, ihre Sicherheit oder ihre Grundrechte betreffen.

Liegen die oben genannten Voraussetzungen vor, dann kann die betroffene Person nach Art. 86 Abs. 1 KI-VO vom Betreiber „eine klare und aussagekräftige Erläuterung zur Rolle des KI-Systems im Entscheidungsprozess und zu den wichtigsten Elementen der getroffenen Entscheidung“ verlangen.

1. Anspruchsgegner

Betreiber[24] im Sinne der KI-VO ist die Person, die ein KI-System[25] in eigener Verantwortung verwendet. Ausgenommen sind Fälle, in denen das KI-System im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet wird (Art. 3 Nr. 4 KI-VO). In eigener Verantwortung bedeutet, dass die Person „auf eigene Rechnung und auf eigenes Risiko“ handelt.[26] Betreiber ist somit nicht mit dem (End-)Nutzer gleichzusetzen.[27] Wenn Angestellte ein KI-System für ihre:n Arbeitgebende:n einsetzen, dann ist der:die Arbeitgebende als Betreiber:in anzusehen.[28] Der Benutzer ist daher nicht gleichzusetzen mit der Person, die das KI-System bedient.[29] Eine Person kann Betreiber und Anbieter gleichzeitig sein.[30]

Setzt eine Behörde ein KI-System ein, ist fraglich, wer als Betreiber anzusehen ist. Betreiber kann nach dem ausdrücklichen Wortlaut des Art. 3 Nr. 4 KI-VO nämlich sowohl eine juristische Person als auch eine Behörde sein. Darin wird teilweise eine Friktion mit dem deutschen Rechtsträgerprinzip gesehen.[31] Juristische Personen des öffentlichen Rechts sind Körperschaften, Anstalten und Stiftungen.[32] Hinter einer Behörde können mehrere Rechtsträger stehen.[33] Anders als die DSGVO, kennt die KI-VO keine „gemeinsamen Betreiber“. Eine Pflicht, die Art. 26 DSGVO entsprechen würde, fehlt in der KI-VO. Daher stellt sich im Verwaltungsrecht beim Einsatz von KI-Systemen regelmäßig die Frage, ob die Behörde oder die juristische Person (des öffentlichen Rechts) Betreiberin im Sinne der KI-VO ist.

Hochschulen sind in der Regel Körperschaften des öffentlichen Rechts und zugleich staatliche Einrichtungen.[34] Sie können

23 Zu den relevanten Hochrisiko-KI-Systemen siehe Schöbel, Der AI Act und die Wissenschaft, DFN-Infobrief Recht 2/2025, S. 3 f.

24 Im Englischen als „deployer“ bezeichnet.

25 Der Begriff des KI-Systems wird in Art. 3 Nr. 1 KI-VO legaldefiniert. Siehe dazu Schöbel, AI Act – Licht der Europäischen Union? DFN-Infobrief Recht 12/2024, S. 8.

26 Wendehorst, in: Martini/Wendehorst, KI-VO, 2024, Art. 3 Rn. 84.

27 Kirschke-Biller/Füllsack, in: BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Art. 3 Rn. 98.

28 Wendehorst, in: Martini/Wendehorst, KI-VO, 2024 Art. 3, Rn. 84.

29 Kirschke-Biller/Füllsack, in: BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Art. 3 Rn. 101.

30 Kirschke-Biller/Füllsack, in: BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Art. 3 Rn. 102; Wendehorst, in: Martini/Wendehorst, KI-VO, 2024, Art. 3 Rn. 86

31 Kirschke-Biller/Füllsack, in: BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Art. 3 Rn. 115.

32 Vgl. Maurer/Waldhoff, Allgemeines Verwaltungsrecht, § 21 Rn. 8.

33 Vgl. Meissner/Schenk, in: Schoch/Schneider (Hrsg.), 47. EL Februar 2025, VwGO § 78 Rn. 37.

34 Vgl. § 58 Abs. 1 S. 1 HRG, § 2 Abs. 1 S. 1 BerlHG, § 5 Abs. 1 S. 1 BbG HG, § 4 S. 1 Nr. 2 BayHSchG, § 8 Abs. 1 S. 1 LHG BaWü, § 2 Abs. 1 S. 1 BremHG, § 2 Abs. 1 S. 1 HmbHG, § 1 Abs. 1 HessHG, § 1 Abs. 1 S. 1 LHG M-V, § 15 S. 1 NHG, § 2 Abs. 1 S. 1 HG NRW, § 2 Abs. 1 S. 1 KunstHG NRW, § 6 Abs. 1 S. 1 HochSchG RLP, § 2 Abs. 1 S. 1 SHSG, § 6 Abs. 1 S. 1 SaarlMhG, § 6 Abs. 1 S. 1 SaarlKhG, § 2 Abs. 1 SächsHSG, § 54 Abs. 1 S. 1 HSG LSA, § 2 Abs. 1 S. 2 HSG S H, § 2 Abs. 1 ThürHG.

auch in anderen Rechtsformen, etwa als Stiftungen, errichtet werden (§ 58 Abs. 1 S. 2 Hochschulrahmengesetz (HRG)). Als Körperschaften des öffentlichen Rechts, Anstalten oder Stiftungen sind sie juristische Personen und können Betreiber von KI-Systemen sein. Fakultäten und Fachbereiche sind zwar teilrechtsfähige Körperschaften, aber selbst keine juristische Person des öffentlichen Rechts.[35] Daher liegt es nahe, dass Betreiber eines KI-Systems im Sinne der KI-VO die Hochschule und nicht etwa eine bestimmte Fakultät ist. Setzen mehrere Fakultäten gemeinsam ein KI-System ein, kommt es daher nicht zu einer Mehrheit von potenziellen Betreibern.

2. Hochrisiko-KI-System

Bei dem KI-System muss es sich um ein Hochrisiko-KI-System nach Art. 6 Abs. 2 i. V. m. Anhang III KI-VO handeln. Hochrisiko-KI-Systeme nach Art. 6 Abs. 1 i. V. m. Anhang I KI-VO fallen demnach nicht in den Anwendungsbereich des Art. 86 KI-VO. Zudem sind solche Hochrisiko-KI-Systeme nicht erfasst, die unter Anhang III Nr. 2 KI-VO fallen. Dies sind KI-Systeme, die bestimmungsgemäß als Sicherheitsbauteile im Rahmen der Verwaltung und des Betriebs kritischer digitaler Infrastruktur, des Straßenverkehrs oder der Wasser-, Gas-, Wärme- oder Stromversorgung verwendet werden sollen.
Für den Hochschulsektor dürften insbesondere zwei aufgeführte Bereiche des Anhangs III relevant sein. Das sind allgemeine und berufliche Bildung (Anhang III Nr. 3 KI-VO) sowie Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit (Anhang III Nr. 4 KI-VO). Allgemeine und berufliche Bildung erfasst auch universitäre Bildung.[36] Im Bereich der allgemeinen und beruflichen Bildung sind etwa KI-Systeme erfasst, die für Zugang und Zulassung verwendet werden sollen. Auch die KI-gestützte Bewertung von Lernergebnissen fällt in diesen Bereich. Fraglich ist, ob auch Systeme, die zur Überwachung und Erkennung von verbotenem Verhalten in Hochschulen eingesetzt werden, erfasst sind. Die deutsche Sprachfassung spricht hier von „Schülern“, die englische Sprachfassung hingegen von „students“.

Im Bereich der Beschäftigung und des Personalmanagements fallen solche KI-Systeme in den Anwendungsbereich, die für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen. Dies schließt die Schaltung gezielter Stellenanzeigen, das Filtern und Sichten von Bewerbungen und die Bewertung von Bewerber:innen ein. Werden KI-Systeme in Entscheidungen, die Bedingungen von Arbeitsverhältnissen, Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen beeinflussen, eingesetzt, so handelt es sich ebenfalls um Hochrisiko-KI-Systeme.

Betroffene müssen über den Einsatz von Hochrisiko-KI-Systemen informiert werden (Art. 26 Abs. 11 S. 1 KI-VO). Dass eine Entscheidung mittels KI getroffen wird oder durch KI unterstützt wird, muss der Person, die diese Entscheidung betrifft, also schon nach Art. 26 Abs. 11 KI-VO mitgeteilt werden. Vor der Verwendung eines Hochrisiko-KI-Systems am Arbeitsplatz müssen die Arbeitgeber, die Arbeitnehmervertreter und die betroffenen Arbeitnehmer darüber informieren, soweit diese der Verwendung des Systems unterliegen (Art. 26 Abs. 7 KI-VO).[37] Art. 26 KI-VO regelt die Information über das „Ob“ und Art. 86 KI-VO regelt die Information über das „Wie“ der Entscheidungsbeteiligung des KI-Systems.[38]

3. Entscheidung

Eine Entscheidung muss auf Grundlage der Ausgabe eines KI-Systems getroffen worden sein. Erwägungsgrund 171 KI-VO spricht davon, dass die Entscheidung überwiegend auf der Ausgabe eines KI-Systems beruht. Der Wortlaut von Art. 86 KI-VO enthält keine Vorgabe. Im Gegensatz zu Art. 22 DSGVO verlangt Art. 86 KI-VO gerade nicht, dass die Entscheidung autonom oder ausschließlich automatisiert erfolgen muss.[39] Daher soll es bereits ausreichen, wenn einer menschlichen Entscheidung KI-generierte Informationen und Daten zugrunde liegen.[40] Darin liegt ein bedeutender Unterschied zum Recht auf Erklärung nach der DSGVO.

35 Maurer/Waldhoff, Allgemeines Verwaltungsrecht, § 21 Rn. 10.

36 Klawonn, in: BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Anhang III Rn. 48.

37 Vgl. Merkle, Transparenz nach der KI-Verordnung – von der Blackbox zum Open-Book?, RDi 2024, 414, 419.

38 Hilgendorf/Härtlein, in: HK-KI-VO, Art. 86 Rn. 4.

39 Hartmann in: Martini/Wendehorst, KI-VO, 2024, Art. 86, Rn. 10.

40 Hartmann in: Martini/Wendehorst, KI-VO, 2024, Art. 86, Rn. 10.

4. Klare und aussagekräftige Erläuterung

Die Erläuterung ist aussagekräftig, wenn sie relevante Informationen in einem ausreichenden Detaillierungsgrad enthält.[41] Nach Art. 86 Abs. 1 KI-VO umfasst sie zwei Teile: die Rolle des KI-Systems im Entscheidungsprozess und die wichtigsten Elemente der getroffenen Entscheidung.
Der erste Teil bezieht sich auf die jeweiligen Verursachungsbeiträge an der Entscheidung von Mensch und Maschine.[42] Die folgenden vier Teile sollen umfasst sein: Beschaffenheit der KI, Zweck der KI, Einfluss der KI auf den Entscheidungsprozess und die Einflüsse auf die KI selbst.[43] Die wichtigsten Elemente der getroffenen Entscheidung enthalten alle Faktoren, auf denen die Entscheidung beruht.[44]

5. Anspruchsinhaber

Den Anspruch hat die Person, die von der Entscheidung betroffen ist.[45] Sind mehrere Personen von einer Entscheidung betroffen, dann sind diese auch Anspruchsinhaber:innen. Betroffen können auch die Personen sein, die nicht Adressaten der Entscheidung sind.[46] Bisher nicht abschließend geklärt ist, ob das Recht nur natürlichen oder auch juristischen Personen zusteht.[47] Im Hochschulkontext dürfte das Recht auf Erläuterung aber vor allem für natürliche Personen relevant sein.

6. Ausnahmen und Subsidiarität

Das Recht nach Art. 86 Abs. 1 KI-VO gilt nur, soweit im Unionsrecht oder dem Recht der Mitgliedstaaten keine Abweichungen vorgesehen sind (Art. 86 Abs. 2 KI-VO). Ausnahmen von diesem Recht enthalten etwa Art. 23 DSGVO, Art. 15 JI-RL,[48] Art. 25 VO (EU) 2018/1725[49] und § 39 Abs. 2 Nr. 3 Alt. 2 VwVfG.[50]

Nach Art. 86 Abs. 3 KI-VO gilt das Recht auf Erläuterung aus der KI-VO nur, soweit dieses Recht nicht anderweitig im Unionsrecht festgelegt ist. Die Vorschrift regelt also Fälle der Normkonkurrenz.[51] Es genügt dabei nicht, dass die Vorschrift aus dem nationalen Recht eines Mitgliedstaates herrührt.[52] Art. 86 Abs. 1 KI-VO tritt zudem nur dann zurück, wenn eine anwendbare Vorschrift eine vergleichbare Rechtsfolge herbeiführt.[53] Besonders relevant ist gerade die Abgrenzung von Art. 13-15 i. V. m. Art. 22 DSGVO und Art. 86 Abs. 1 KI-VO. Ein wesentlicher Unterschied ist, dass es nach Art. 86 KI-VO ausreicht, wenn die Entscheidung auf der Grundlage einer mittels Hochrisiko-KI-System generierten Ausgabe und nicht auf einer automatisierten Verarbeitung

---

41 Djeffal in:BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Art. 86 Rn. 31.

42 Merkle, Transparenz nach der KI-Verordnung – von der Blackbox zum Open-Book?, RDi 2024, 414, 419.

43 Djeffal in:BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Art. 86 Rn. 32.

44 Hartmann in: Martini/Wendehorst, KI-VO, 2024, Art. 86, Rn. 15.

45 Hartmann in: Martini/Wendehorst, KI-VO, 2024, Art. 86, Rn. 12.

46 Djeffal in:BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Art. 86 Rn. 19.

47 Hartmann in: Martini/Wendehorst, KI-VO, 2024, Art. 86, Rn. 12.

48 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 S. 89.

49 Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, ABl. L 295 S. 39.

50 Djeffal, in:BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Art. 86 Rn. 40.

51 Djeffal, in:BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Art. 86 Rn. 42.

52 Hartmann, in: Martini/Wendehorst, KI-VO, 2024, Art. 86 Rn. 17.

53 Hartmann, in: Martini/Wendehorst, KI-VO, 2024, Art. 86 Rn. 17.

erfolgt. Hier ist der Anwendungsbereich des Art. 86 Abs. 1 KI-VO also weiter als das Recht auf Erklärung aus der DSGVO.[54] Eine Einschränkung im Vergleich zur DSGVO macht Art. 86 Abs. 1 KI-VO allerdings dadurch, dass die Ausgabe von einem Hochrisiko-KI-System stammen muss – was nach der DSGVO gerade nicht der Fall sein muss.[55]

IV. Ausblick

Sowohl die DSGVO als auch die KI-VO sehen ein Recht auf Erklärung bzw. Erläuterung vor. Die jeweiligen Ansprüche sind dabei aber nicht deckungsgleich. Der Einsatz von KI im Hochschulkontext kann dazu führen, dass Hochschulen den betroffenen Personen die eingesetzte KI erklären müssen. Wie umfangreich der rechtliche Anspruch der DSGVO nach der Rechtsprechung des EuGH ist, wird in einer kommenden Ausgabe geklärt. Die Verpflichtungen über Hochrisiko-KI-Systeme nach der KI-VO gelten erst ab dem 2. August 2026. Daher gibt es bislang noch keine Rechtsprechung zum Recht auf Erläuterung nach Art. 86 KI-VO.

Die Pflicht zur Erklärung einer hoheitlichen Entscheidung kann sich auch aus den Normen des nationalen Verwaltungsrechts ergeben. Soweit es sich bei der Entscheidung um einen Verwaltungsakt im Sinne des § 35 S. 1 Verwaltungsverfahrensgesetz (VwVfG) handelt, kann es erforderlich sein, dass dieser begründet wird. Ein schriftlicher oder elektronischer sowie ein schriftlich oder elektronisch bestätigter Verwaltungsakt sind mit einer Begründung zu versehen (§ 39 Abs. 1 S. 1 VwVfG). Inhalt der Begründung müssen auch die wesentlichen tatsächlichen Gründe sein, die die Behörde zu ihrer Entscheidung bewogen haben (§ 39 Abs. 1 S. 2 VwVfG). Fraglich ist, ob daraus auch ein Recht auf Erklärung von KI folgt. Dieser Frage wird ebenfalls in einem kommenden Beitrag nachgegangen.

54 Vgl. Hartmann, in: Martini/Wendehorst, KI-VO, 2024, Art. 86 Rn. 17; Djeffal, in: BeckOK KI-Recht, 2. Ed. 1.5.2025, KI-VO Art. 86 Rn. 44.

55 Vgl. Hartmann, in: Martini/Wendehorst, KI-VO, 2024, Art. 86 Rn. 17.

Ohne Widerspruch ist alles erlaubt

OLG Köln zur Rechtmäßigkeit des Trainings von KI-Modellen mit personenbezogenen Daten

Von Johannes Müller-Westphal, Münster

Bei dem Training von KI-Modellen werden häufig auch personenbezogene Daten verarbeitet. Hierbei stellt sich die Frage, ob die Datenverarbeitung rechtmäßig im Sinne der Datenschutz-Grundverordnung (DSGVO) ist. Das Oberlandesgericht (OLG) Köln musste sich in seinem Beschluss vom 23. Mai 2025 im Eilverfahren (Az. 15 UKl 2/25) mit der Frage beschäftigen, ob Meta Platforms öffentlich zugängliche Beiträge von Nutzern der Meta-Plattformen zur Verbesserung eigener KI-Modelle verwenden darf.

I. Training von KI-Modellen mit personenbezogenen Daten

Große Sprachmodelle (LLMs) sollen imstande sein, auf die Eingabe der Nutzer adäquat zu reagieren und die vom Nutzer gewünschten Texte zu verfassen. Maßgeblich für diese Fähigkeit sind neben der Architektur des Sprachmodells vor allem die Daten, mit denen das Modell trainiert wurde. Im Rahmen des Trainings soll das Sprachmodell in den Daten Muster erkennen, die es später verwenden kann, um auf die Eingabe der Nutzer zu reagieren. Hierfür wird eine große Menge an Daten benötigt. Für Sprachmodelle müssen die Trainingsdaten Texte enthalten. Um die erforderliche große Menge an Textdaten zu erhalten, greifen KI-Anbieter häufig auf Texte zurück, die im Internet frei verfügbar sind.[1] Die Informationen, die in diesen Textdaten enthalten sind, können sich regelmäßig auch auf identifizierte oder identifizierbare Personen beziehen. In diesem Fall müssen zum KI-Training personenbezogene Daten verarbeitet werden, sodass der Anwendungsbereich der DSGVO eröffnet ist.[2]

Die DSGVO verlangt für die Verarbeitung personenbezogener Daten insbesondere, dass diese rechtmäßig sein muss, also von einem der Erlaubnistatbestände in Art. 6 Abs. 1 DSGVO gedeckt ist. Besonders viele Datenverarbeitungen stützen sich auf Art. 6 Abs. 1 lit. a DSGVO. Hierfür muss die betroffene Person, auf die sich die verarbeiteten Daten beziehen, eine Einwilligung in die Datenverarbeitung zu dem spezifischen Zweck erteilen. Im Fall des Trainings von KI-Modellen mit personenbezogenen Daten erweist sich der Rechtfertigungstatbestand aber nicht als besonders praktikabel. Bei frei verfügbaren Daten im Internet müsste die Daten verarbeitende Stelle alle Personen identifizieren und um ihre Einwilligung in die Datenverarbeitung zu Zwecken des KI-Trainings bitten. Bereits die Identifikation und Benachrichtigung der betroffenen Personen wird in den meisten Fällen nicht möglich sein. Sofern eine Einrichtung ohne Einwilligung der betroffenen Person ihre Daten zum KI-Training verwendet, wird sie sich in der Regel auf den Erlaubnistatbestand in Art. 6 Abs. 1 lit. f DSGVO stützen. Hiernach ist eine Datenverarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen, Grundrechte oder Grundfreiheiten der betroffenen Person überwiegen.[3] Der Erlaubnistatbestand erfordert eine

1 Siehe hierzu auch Müller, Die Menge macht's, DFN-Infobrief Recht 11/2024.

2 Von der Thematik des datenschutzkonformen Trainings von KI-Modellen ist die Frage getrennt zu betrachten, ob KI-Modelle nicht nur mit personenbezogenen Daten trainiert wurden, sondern diese nach dem Training auch in dem Modell enthalten sind, also ob das Modell personenbezogene Daten „gespeichert" hat. Hierzu Müller, Das kann sich doch niemand merken, DFN-Infobrief Recht 03/2025. Zu dieser Frage hat auch der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Stellung bezogen. Sein Diskussionspaper ist abrufbar unter https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf (alle Links des Beitrags zuletzt abgerufen am 18.09.2025).

3 Ausführlich zu dem Erlaubnistatbestand Müller, Damit konnte doch keiner rechnen, DFN-Infobrief Recht 01/2025.

Abwägung der Interessen des Verantwortlichen, der über die Datenverarbeitung entscheidet, und der betroffenen Person, auf die sich die Daten beziehen. Dadurch ist er mit einer erhöhten Rechtsunsicherheit verbunden. Sofern sich die Entwickler eines KI-Modells für das Training mit personenbezogenen Daten auf Art. 6 Abs. 1 lit. f DSGVO berufen, besteht auch für sie eine große Unsicherheit, ob die Datenverarbeitung tatsächlich hiervon gedeckt ist und ein Gericht im Fall eines etwaigen Verfahrens von einer rechtmäßigen Datenverarbeitung ausgehen würde. Bei der Prüfung von Art. 6 Abs. 1 lit. f DSGVO ist gemäß dem Erwägungsgrund 47 zur DSGVO insbesondere zu berücksichtigen, ob die betroffene Person die Datenverarbeitung zu dem konkreten Zweck vernünftigerweise erwarten konnte. Darüber hinaus ist relevant, welche negativen Auswirkungen sich für die betroffene Person aus der Datenverarbeitung ergeben.[4]

Bei bestimmten Kategorien von personenbezogenen Daten, die als besonders sensibel gelten, gelten zudem erhöhte Verarbeitungsanforderungen. Diese sind in Art. 9 DSGVO normiert.[5] Zu diesen besonders sensiblen Daten zählen insbesondere Gesundheitsdaten. Art. 9 Abs. 2 DSGVO nennt die Voraussetzungen, unter denen diese Daten verarbeitet werden dürfen. Möglich ist eine Verarbeitung etwa bei Vorliegen einer ausdrücklichen Einwilligung der betroffenen Person (Art. 9 Abs. 2 lit. a DSGVO). Art. 9 DSGVO enthält aber keinen Erlaubnistatbestand, der dem in Art. 6 Abs. 1 lit. f DSGVO nahekommt. Die Verarbeitung der besonders sensiblen Daten kann damit nicht mit der Begründung legitimiert werden, dass der Verantwortliche ein berechtigtes Interesse an der Datenverarbeitung hat, das nicht von den Interessen des Betroffenen überwogen wird.

Sofern im Internet frei verfügbare Texte zum KI-Training verwendet werden, ist die Wahrscheinlichkeit hoch, dass diese auch personenbezogene Daten enthalten können, die unter Art. 9 DSGVO fallen. Auch hier wird regelmäßig keine Einwilligung der betroffenen Person eingeholt werden, sodass die Datenverarbeitung nicht von Art. 9 Abs. 2 lit. a DSGVO legitimiert werden kann. Teilweise erlauben die anderen Erlaubnistatbestände in Art. 9 Abs. 2 DSGVO die Datenverarbeitung, soweit anderes Unionsrecht oder das Recht eines Mitgliedstaats die Datenverarbeitung zu dem spezifischen Zweck erlaubt. Hierfür braucht es aber eine weitere Regelung und eine solche ist auch nur für den Fall möglich, dass die Datenverarbeitung aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist (Art. 9 Abs. 2 lit. g DSGVO) oder die Datenverarbeitung für im öffentlichen Interesse liegende Archivzwecke oder wissenschaftliche oder historische Forschungszwecke erfolgt (Art. 9 Abs. 2 lit. j DSGVO). Von den weiteren Erlaubnistatbeständen des Art. 9 Abs. 2 DSGVO kommt für den Fall des KI-Trainings regelmäßig noch Art. 9 Abs. 2 lit. e DSGVO in Betracht. Hiernach ist eine Datenverarbeitung erlaubt, wenn sie sich auf personenbezogene Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat. Wurden die Daten, die zum Training einer KI verwendet werden, jedoch durch eine andere Person als die betroffene Person im Internet veröffentlicht, scheidet Art. 9 Abs. 2 lit. e DSGVO als Legitimationsgrund aus.

Insgesamt bestehen also zahlreiche offene Fragen zu der datenschutzrechtlichen Rechtfertigung des Trainings von KI mit personenbezogenen Daten. Nun hat sich das OLG Köln in seinem Beschluss vom 23.05.2025 (Az. 15 UKl 2/25) mit mehreren dieser Fragen auseinandergesetzt. Soweit ersichtlich liegt hierin eine der ersten umfangreichen Auseinandersetzungen eines deutschen Gerichts mit der Frage nach der datenschutzrechtlichen Rechtmäßigkeit des Trainings von KI-Modellen mit personenbezogenen Daten.

II. Verbraucherzentrale Nordrhein-Westfalen vs. Meta

Der Konzern Meta Platforms Ireland – Betreiberin von Facebook und Instagram in Europa – kündigte am 14. April 2025 an, ab dem 27. Mai 2025 öffentlich eingestellte personenbezogene Daten von volljährigen Nutzern zum Training und zur Verbesserung eigener KI-Modelle zu verarbeiten. Meta unterschied dabei zwischen zwei Datenkategorien: sogenannte „First-Party-Daten", also Inhalte, die Nutzer selbst öffentlich einstellen – darunter Profilbilder, öffentliche Kommentare und Bewertungen, öffentliche Instagram-Posts sowie die dazugehörigen Metadaten – und sogenannte „Flywheel-Daten", also Nutzungsdaten, die bei Interaktionen der Nutzer mit Metas KI-Funktionen entstehen,

4 Hierauf stellt auch der EuGH explizit ab, etwa in seinem Urteil vom 04.07.2023 (Az. C-252/21).

5 Siehe zur Verarbeitung besonders sensibler Gesundheitsdaten Geiselmann, DigiG und GDNG – Der Doppelwumms zum digitalen Gesundheitswesen, DFN-Infobrief Recht 05/2024; Müller, GENehmigte Datennutzung, DFN-Infobrief Recht 07/2024; Müller, Datenschutz auf Rezept, DFN-Infobrief Recht 02/2023.

etwa durch Chatbots oder Bildgeneratoren. Im Verfahren ging es zuletzt nur noch um die First-Party-Daten.

Die Verbraucherzentrale Nordrhein-Westfalen ging von der Rechtswidrigkeit der angekündigten Tätigkeiten aus und beantragte in einem Eilverfahren, Meta in Form einer einstweiligen Verfügung zu untersagen, öffentlich eingestellte personenbezogene Daten erwachsener Nutzer zum Training und zur Verbesserung eigener KI-Modelle zu verarbeiten.

Meta betonte, man habe im Vorfeld eng mit der zuständigen irischen Datenschutzaufsichtsbehörde zusammengearbeitet und auch die Stellungnahme des Europäischen Datenschutzausschusses (EDSA) berücksichtigt. Als technische und organisatorische Schutzmaßnahmen seien Verfahren zur teilweisen Deidentifizierung der Daten eingeführt worden. Zudem werde allen betroffenen Nutzern ein Widerspruchsrecht („Opt-out“) eingeräumt, um die Nutzung ihrer Inhalte zu verhindern. Die irische Datenschutzaufsichtsbehörde untersagte die geplante Verarbeitung nicht, forderte Meta jedoch auf, im Oktober 2025 einen Bericht über die Wirksamkeit der Maßnahmen vorzulegen.

III. Beschluss des OLG Köln

Das OLG Köln musste sich mit möglichen Verstößen von Meta gegen den Digital Markets Act (DMA) und die DSGVO auseinandersetzen. Die Vorschriften des DMA waren aber nur in dem Verfahren relevant, weil es sich bei Meta um einen sogenannten Torwächter handelt, also einen Plattformdienst, der über eine besondere Marktmacht verfügt. Die Ausführungen sind aber insbesondere für wissenschaftliche Einrichtungen nicht relevant. Nachfolgend sollen daher lediglich die Erwägungen zur DSGVO-Konformität dargestellt werden.

1. Überwiegende berechtigte Interessen nach Art. 6 Abs. 1 lit. f DSGVO

Das Gericht prüfte zunächst, ob sich Meta auf die Rechtsgrundlage „berechtigtes Interesse“ nach Art. 6 Abs. 1 lit. f DSGVO stützen darf, wenn es öffentlich sichtbare Inhalte für das Training seiner KI-Modelle verwendet, ohne vorher die Einwilligung der Betroffenen einzuholen. Eine speziellere gesetzliche Grundlage sah das Gericht nicht. Nach dem für Art. 6 Abs. 1 lit. f DSGVO erforderlichen Dreischritt prüfte das OLG Köln, ob Meta ein berechtigtes Interesse verfolgt, ob die Datenverarbeitung hierfür erforderlich ist und ob die Interessen der betroffenen Person nicht überwiegen.[6]

Als Erstes stellte das Gericht fest, dass Metas Ziel – die Entwicklung und Verbesserung generativer KI – grundsätzlich ein berechtigtes wirtschaftliches Interesse ist.

Im zweiten Schritt prüfte das Gericht, ob die Verarbeitung „erforderlich“ ist, um dieses Ziel zu erreichen. Hierfür muss sie geeignet sein, und es darf kein anderes, genauso wirksames, aber weniger eingreifendes Mittel geben. Es nahm an, dass Meta glaubhaft gemacht hatte, dass große KI-Modelle sehr große und vielfältige Datenmengen brauchen – auch mit regionalen Besonderheiten – und dass allein die sogenannten Flywheel-Daten (aus KI-Interaktionen) oder rein synthetische Daten dafür nicht ausreichen. Auch eine vollständige Anonymisierung würde die Daten stark entwerten. Das Gericht folgte diesem Vortrag und sah keine gleichwertige Alternative. Hierbei wertete das Gericht positiv, dass Meta die Daten teilweise deidentifiziert (z. B. Entfernen von Namen, E-Mail-Adressen, Telefonnummern) und sie in einem unstrukturierten Format speichert.

Im dritten Schritt nahm das Gericht eine Interessenabwägung vor. Hierbei stellte das Gericht unter anderem auf die legitimen Erwartungen der Nutzer ab. Nutzer, die nach dem 26. Juni 2024 Inhalte öffentlich eingestellt haben, konnten laut Gericht damit rechnen, dass Meta diese auch fürs KI-Training nutzt – denn zu diesem Zeitpunkt hatte Meta schon offen über seine Pläne informiert. Für Inhalte, die davor veröffentlicht wurden, sah das Gericht diese Erwartbarkeit zwar nicht. Allerdings könnten Nutzer jederzeit widersprechen oder ihre Inhalte „entöffentlichen“, sodass sie nicht mehr für das Training genutzt würden. Der Möglichkeit zum Widerspruch und zur Entöffentlichung maß das OLG Köln eine besondere Bedeutung zu. Das Gericht berücksichtigte außerdem, dass die jeweiligen Inhalte bereits öffentlich zugänglich und damit oft sogar über Suchmaschinen auffindbar sind. Gleichzeitig berücksichtigte das Gericht positiv, dass Meta Maßnahmen zur Deidentifizierung der betroffenen Person ergriffen hat. Besonders stark stellte das Gericht auf die tatsächlichen Risiken ab, die durch das KI-Training entstehen. Hierbei ging es davon aus, dass es unwahrscheinlich

6 Hierzu EuGH, Urteil vom 04.07.2023 (Az. C-252/21).

sei, dass durch die Verarbeitung ein konkreter Nachteil für die betroffene Person entstehen könnte. Eine Gefahr könne allein darin bestehen, dass die Daten durch die Ausgabe der KI später wiedergegeben werden könnten. Diese Gefahr sei aber insgesamt niedrig. Daher nahm das Gericht eine Rechtfertigung der Datenverarbeitung zu Trainingszwecken gemäß Art. 6 Abs. 1 lit. f DSGVO an. Aufgrund der geringen Identifizierungswahrscheinlichkeit von Einzelpersonen ging das OLG Köln dabei auch davon aus, dass auch Datenverarbeitungen, die sich auf dritte Personen beziehen, die die Daten nicht selbst veröffentlicht haben, gemäß Art. 6 Abs. 1 lit. f DSGVO gerechtfertigt sind.

2. Art. 9 DSGVO

Zudem beschäftigte sich das OLG Köln mit der Rechtmäßigkeit der Verarbeitung besonders sensibler Daten gemäß Art. 9 DSGVO. Das Gericht ging davon aus, dass solche Informationen im geplanten Trainingsdatensatz von Meta durchaus enthalten sein können.

Das Gericht prüfte vor allem die Ausnahme nach Art. 9 Abs. 2 lit. e DSGVO, die die Verarbeitung erlaubt, wenn die betroffene Person die sensiblen Daten offensichtlich selbst öffentlich gemacht hat. Das OLG Köln führte aus, dass die Ausnahme nur greife, wenn ein Nutzer freiwillig eigene sensible Angaben – zum Beispiel über die Gesundheit oder politische Ansichten – öffentlich gepostet hat.[7] Dabei muss es sich klar erkennbar um ein „Öffentlichmachen" handeln, das bewusst erfolgt.

Bei sensiblen Daten, die sich auf andere Personen beziehen, die die Daten selbst nicht öffentlich gemacht haben, greift diese Ausnahme nicht. An dieser Stelle führte das Gericht aus, dass es im Hauptverfahren prüfen werde, die Frage der Rechtmäßigkeit der Datenverarbeitung dem EuGH zur Vorabentscheidung vorzulegen. In dem vorliegenden Eilverfahren sei eine solche Prüfung nicht möglich. Hier ging das OLG Köln davon aus, dass ein Verarbeitungsverbot erst auf Antrag der betroffenen Person greift. Das Gericht stützt diese Einschätzung auf Überlegungen aus der Rechtsprechung des EuGH zu Suchmaschinen (Rs. C-136/17), wo ebenfalls zwischen potenziell rechtswidrigen Inhalten und einem individuellen Löschbegehren unterschieden wurde.

Damit lehnte das OLG Köln eine wortgetreue Anwendung des Art. 9 DSGVO für den Fall ab, dass die sensiblen Daten nicht zielgerichtet zum Training von KI-Modellen verarbeitet werden. Das Gericht nahm dabei an, dass der europäische Verordnungsgeber in der KI-VO zum Ausdruck gebracht habe, dass das Training von KI mit riesigen Mengen an Daten, die im Internet frei verfügbar sind, rechtmäßig sein könne. Dies sei aber nur möglich, wenn Art. 9 DSGVO nicht streng wortgetreu angewandt werde.

IV. Relevanz weiterer Gerichtsentscheidungen

Es gilt zu beachten, dass es sich bei der Entscheidung lediglich um den Beschluss eines einzelnen Gerichts handelt. Es ist nicht unwahrscheinlich, dass andere Gerichte die Datenschutzkonformität des KI-Trainings mit personenbezogenen Daten anders einschätzen könnten. Dies hat jüngst das OLG Schleswig-Holstein in seinem Beschluss vom 12.08.2025 (Az. 6 UKl 3/25) angedeutet. In diesem ging es um denselben Sachverhalt des KI-Trainings mit personenbezogenen Daten durch Meta. Antragstellerin war eine Stiftung zum Schutz von Verbraucherinteressen. In dem Beschluss wurde der Antrag auf einstweiligen Rechtsschutz abgelehnt, da dem Begehren die erforderliche Dringlichkeit fehlte. Der Verband ließ trotz Kenntnis von den beabsichtigten Datenverarbeitungen durch Meta zunächst einen zu langen Zeitraum verstreichen. Daher setzte sich das Gericht auch nur in einem sehr begrenzten Umfang mit der Frage der Rechtmäßigkeit der Datenverarbeitung auseinander. Hierbei deutete es jedoch an, dass die Datenverarbeitung von besonders sensiblen Daten nach Art. 9 DSGVO grundsätzlich rechtswidrig sei, sofern sich die Daten auf Personen beziehen, die nicht auf der jeweiligen Plattform registriert seien, und die Daten von registrierten Nutzern hochgeladen wurden. Eine Ausnahme von diesem Grundsatz im Fall des nicht zielgerichteten KI-Trainings ließ das OLG Schleswig-Holstein in seiner sehr kurzen Auseinandersetzung nicht erkennen.

V. Relevanz für wissenschaftliche Einrichtungen

Der Frage der Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu Zwecken des KI-Trainings kommt hohe Relevanz

7 Hierzu auch EuGH, Urteil vom 04.07.2023 (Az. C-252/21).

für all diejenigen wissenschaftlichen Einrichtungen zu, die eigene KI-Modelle selbst entwickeln. Das OLG Köln zeigt dabei auf, dass auch ein Training mit personenbezogenen Daten datenschutzkonform erfolgen kann. Insbesondere die datenschutzrechtlich besonders herausfordernde Konstellation der Verarbeitung personenbezogener Daten, die die Betroffenen nicht selbst öffentlich gemacht haben, betrachtete das OLG Köln nicht per se als rechtswidrig. Besonders hervorzuheben ist, dass das OLG Köln darauf abstellte, ob für die betroffene Person tatsächliche Risiken durch das Training mit ihren Daten drohen, vor allem in Form einer späteren Ausgabe der persönlichen Informationen. Dieses Risiko sollten auch wissenschaftliche Einrichtungen minimieren, indem sie wirksame Deidentifizierungsmaßnahmen ergreifen.

Gleichzeitig muss berücksichtigt werden, dass andere Gerichte das Training von KI-Modellen mit personenbezogenen Daten anders bewerten könnten. Eine abschließende Klärung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten, vornehmlich hinsichtlich der Verarbeitung besonders sensibler Daten gemäß Art. 9 DSGVO, findet erst statt, wenn der EuGH hierüber entscheidet. Daher wäre es zu begrüßen, wenn das OLG Köln im Hauptverfahren die entscheidenden Rechtsfragen dem EuGH zur Vorabentscheidung vorlegt.

DFN Infobrief-Recht-Aktuell

• IT-Sicherheitsrecht: Gesetzesentwurf zum KRITIS-Dachgesetz beschlossen

Das Bundeskabinett hat am 10. September 2025 einen Gesetzesentwurf zum KRITIS-Dachgesetz beschlossen. Darin wird festgelegt, welche Infrastruktureinrichtungen unentbehrlich sind, um die Versorgung der Bevölkerung sicherzustellen und die Wirtschaft aufrechtzuerhalten. Zudem werden für die Betreiber dieser Einrichtungen Mindestanforderungen definiert.

Hier erhalten Sie den Link zum Gesetzesentwurf:
https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/KM4/reg-kritis-dachgesetz.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 30.09.2025)

• Datenschutzrecht: Entscheidung des Europäischen Gerichtshofs (EuGH) zur Anonymität von Daten

Mit Urteil vom 4. September 2025 – C-413/23 – hat der EuGH grundlegende Feststellungen zur Anonymität von Daten vorgenommen. Demnach muss die Anonymität oder Personenbeziehbarkeit von Daten aus der Sicht der jeweils verantwortlichen Stelle bestimmt werden. Ein und derselbe Datensatz kann für eine Stelle als personenbezogen zu werten sein, während er für eine andere als anonym einzuordnen ist. Entscheidend ist, ob die jeweilige Stelle über Mittel zur Re-Identifizierung verfügt.

Hier erhalten Sie den Link zur Entscheidung:
https://curia.europa.eu/juris/document/document.jsf?text=&docid=303863&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=16786370 (zuletzt abgerufen am 30.09.2025)

• EU-Recht: Gericht der Europäischen Union (EuG) hält die Gebührenbeschlüsse der EU-Kommission gegen TikTok, Facebook und Instagram für nichtig

Die Europäische Kommission nimmt gegenüber den großen Online-Plattformen nach dem Digital Services Act (DSA) Aufsichtsaufgaben wahr. Zu diesem Zweck werden jährliche Gebühren von diesen Anbietern erhoben, die sich nach der Zahl der Nutzer des jeweiligen Dienstes berechnen. Meta und TikTok wehrten sich gegen die Gebührenbeschlüsse und erhoben Klage beim EuG. Das Gericht erklärte die Beschlüsse daraufhin für nichtig - allerdings lediglich aufgrund eines formellen Fehlers.

Hier erhalten Sie den Link zur Pressemitteilung:
https://curia.europa.eu/jcms/upload/docs/application/pdf/2025-09/cp250114de.pdf (zuletzt abgerufen am 30.09.2025)

Kurzbeitrag: Wird der europäische Datenschutzstandard ausgeschremst?

Das Europäische Gericht (EuG) hält weiter am EU-US Data Privacy Framework fest

von Ole-Christian Tech, Münster

Wenn personenbezogene Daten in Drittländer außerhalb der Europäischen Union übermittelt werden sollen, erfordert dies nach Kapitel 5 der Datenschutz-Grundverordnung (DSGVO) regelmäßig einen Angemessenheitsbeschluss nach Art. 45 DSGVO.[1] Für den praktisch wichtigsten Fall der Datenübermittlung in die USA hat die Europäische Kommission in der Vergangenheit bereits mehrfach versucht, einen Angemessenheitsbeschluss zu schaffen, der diese Datentransfers privilegiert. Sie versuchte es im Juli 2023 erneut mit dem „EU-U.S. Data Privacy Framework" (DPF).[2] Wie seine Vorgänger wurde auch dieser Angemessenheitsbeschluss gerichtlich angefochten. Anders als diese hielt er jedoch einer Überprüfung durch das EuG stand.

I. Hintergrund der Angemessenheitsbeschlüsse

Mit dem sogenannten Angemessenheitsbeschluss nach Art. 45 DSGVO attestiert die Europäische Kommission einem Drittland, dass dieses über einen der DSGVO gleichwertigen Datenschutzstandard verfügt und somit der Europäischen Union für Datentransfers gleichgestellt werden kann. Bereits der historische Kontext des Art. 45 DSGVO ist dabei eng mit der Datenverarbeitung in den USA verknüpft: Die Enthüllungen des Whistleblowers Edward Snowden zu US-Überwachungsprogrammen im Jahr 2013 haben die Rolle der Angemessenheitsbeschlüsse im europäischen Datenschutzrecht maßgeblich geprägt.[3]

II. Bisherige Rechtsprechungslinie des EuGH

In den viel beachteten Verfahren Schrems I und Schrems II, in denen der Datenschutzaktivist Maximilian Schrems die bisherigen Angemessenheitsbeschlüsse zu Fall brachte, hat der Europäische Gerichtshof (EuGH) den normativen Gehalt der „Angemessenheit des gebotenen Schutzniveaus" nach Art. 45 Abs. 2 DSGVO umfassend fortentwickelt.

Dieser stellte in seinem Vorabentscheidungsverfahren fest, dass ein Drittland ein Datenschutzniveau gewährleisten muss, das dem EU-Niveau „der Sache nach gleichwertig" ist. Das im Safe-Harbor-Abkommen vorgesehene System der Selbstzertifizierung von US-Unternehmen erfülle diese Anforderungen nicht. Insbesondere räume das Abkommen den Erfordernissen

1 Derzeit existieren Angemessenheitsbeschlüsse zu insgesamt 15 Staaten, darunter Andorra, Israel, die Schweiz, das Vereinigte Königreich und eben die USA, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=de (alle Links des Beitrags zuletzt abgerufen 30.09.2025).

2 Angemessenheitsentscheidung 2023/1795, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

3 Juarez in: BeckOK Datenschutzrecht Art. 45 Rn. 9; explizit hierzu das Europäische Parlament zum DPF, P9_TA(2023)0204; vertiefend zu den Enthüllungen auch https://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal.

der nationalen Sicherheit und des öffentlichen Interesses der USA unbegrenzten Vorrang gegenüber dem Datenschutzgrundrecht der Betroffenen ein, wodurch Datenverarbeiter verpflichtet waren, die Datenschutzgrundsätze gegenüber den US-Behörden vollständig außer Acht zu lassen. Diese hätten einen generellen, anlasslosen und massenhaften Zugriff auf personenbezogene Daten von EU-Bürgern ohne Differenzierung, Einschränkung oder objektive Kriterien. Zudem monierte das Gericht, dass das völlige Fehlen von Zugangsmöglichkeiten zu den eigenen personenbezogenen Daten sowie von Rechtsbehelfen zur Berichtigung oder Löschung und zu effektivem Rechtsschutz den Wesensgehalt der Grundrechte nach Art. 7, 8 und 47 der EU-Grundrechtecharta (GRCh) verletze. Der EuGH erklärte daraufhin den Angemessenheitsbeschluss „Safe-Harbor" für ungültig.

In der Folge fasste die Europäische Kommission einen zweiten Angemessenheitsbeschluss, das „EU-US Privacy Shield"-Abkommen. In einer ähnlichen Fallkonstellation wandte sich Schrems wieder an die irische Datenschutzbehörde, welche die Beschwerde mit Verweis auf den neuen Angemessenheitsbeschluss zurückwies. Auch hiergegen klagte Schrems vor dem High Court, der die Sache erneut dem EuGH vorlegte.

Das Gericht stellte auch vor dem Hintergrund des neuen Angemessenheitsbeschlusses erhebliche Rechtsschutzlücken fest, die eine Gleichwertigkeit des Datenschutzniveaus der USA gegenüber der EU ausschlossen. Grund dafür waren erneut die auf Section 702 FISA gestützten nachrichtendienstlichen Überwachungsprogramme PRISM und UPSTREAM[4] sowie Programme auf Grundlage der Executive Order 12333.[5] Diese Programme ermöglichten den US-Behörden nach Auffassung des EuGH noch immer, massenhafte, anlasslose Datensammlungen über EU-Bürger, ohne dem Erfordernis der Verhältnismäßigkeit zu genügen.[6]

Gegen diese Grundrechtseingriffe sah das US-Recht für EU-Bürger auch keinen dem europäischen Recht vergleichbaren Rechtsschutz vor. Die im Privacy-Shield-Abkommen vorgesehene Ombudsperson unterstand organisatorisch dem US-Außenministerium – und damit der US-Regierung – und konnte zudem keine verbindlichen Entscheidungen gegenüber den Nachrichtendiensten treffen. Dieser Mechanismus erfüllte daher nicht die Anforderungen an ein unabhängiges und unparteiisches Gericht im Sinne von Art. 47 GRCh.[7] Folglich erklärte der EuGH auch den Angemessenheitsbeschluss Privacy Shield für ungültig.

In Reaktion auf die Kritik des EuGH in den beiden Schrems-Entscheidungen besserten die USA an verschiedenen Stellen nach. Mit der Executive Order 14086 führte US-Präsident Biden im Oktober 2022 grundrechtliche Garantien in Bezug auf die Überwachungstätigkeiten der US-Nachrichtendienste ein. Überwachungsmaßnahmen müssen hiernach auf das „Erforderliche und Verhältnismäßige" beschränkt werden.[8] Daneben erließ der US-Justizminister die Attorney General Regulation No. 5517–2022, die eine gerichtsähnliche Instanz namens Data Protection Review Court (DPRC)[9] einführte. Der neue Rechtsschutzmechanismus ermöglicht es Betroffenen – wie bisher - bei Verdacht einer illegalen Datenverarbeitung durch US-Geheimdienste, eine Beschwerde bei ihrem Datenschutzbeauftragten in der EU einzureichen. Dieser leitet die Beschwerde dann an die US-Regierung weiter, wo der Civil Liberties Protection Officer (CLPO) diese prüft. Dessen Entscheidung ist dann zwar gegenüber den US-Geheimdiensten bindend, wird gegenüber den Betroffenen bzw. Beschwerdeführern jedoch nicht kommuniziert.

Gegen die Entscheidung des CLPO kann der Betroffene dann eine vollständige Nachprüfung durch den Data Protection Review Court (DPRC) beantragen. Dieser setzt sich aus mindestens sechs unabhängigen Juristen mit Sicherheitsfreigabe zusammen, die im Datenschutz- und nationalen Sicherheitsrecht fachkundig sind und ist jedoch kein Gericht im engeren Sinne (Judikative). Es handelt sich dagegen um ein quasigerichtliches Organ innerhalb der Exekutive. Vorschriften, die die Unabhängigkeit und Sicherheit der Richter vor unberechtigter Abberufung schützen, sollen die Vergleichbarkeit zur europäischen Gerichtsbarkeit sicherstellen. Da auch dieses Verfahren geheim ist, können die

4 https://www.intel.gov/foreign-intelligence-surveillance-act/fisa-section-702.

5 https://www.archives.gov/federal-register/codification/executive-order/12333.html.

6 EuGH, Urteil vom 16. Juli 2020, Schrems II, Rs. C 311/18, Rn. 184 (ECLI:EU:C:2020:559).

7 EuGH, Urteil vom 16. Juli 2020, Schrems II, Rs. C 311/18, Rn. 197 (ECLI:EU:C:2020:559).

8 EO 14086, Sec. 2(a)(ii).

9 https://www.justice.gov/opcl/redress-data-protection-review-court.

Beschwerdeführer nicht selbst auftreten, sondern werden von einem Special Advocate vertreten, der aus einem Pool fachkundiger Anwälte stammt, die vom US-Justizminister ernannt werden. Auch die Entscheidung des DPRC ist gegenüber den US-Behörden bindend, wird den Betroffenen aber nicht mitgeteilt.

Schließlich wurde mit dem Privacy and Civil Liberties Oversight Board (PCLOB) ein unabhängiges Gremium mit fünf Mitgliedern geschaffen, das vom Präsidenten ernannt und vom Senat bestätigt wird. Dieses überwacht die Tätigkeiten und Verfahren des CLPO und DPRC und prüft, ob diese unabhängig, rechtzeitig und mit Zugang zu allen nötigen Informationen tätig werden.

III. Das Urteil des EuG

In einem dritten Anlauf fasste die Europäische Kommission dann im Juli 2023 mit dem EU-U.S. Data Privacy Framework einen neuen Angemessenheitsbeschluss. Dieser wurde kurz darauf, am 13. Oktober 2023, vom französischen Abgeordneten Philippe Latombe[10] gerichtlich angefochten. Latombe machte geltend, der Angemessenheitsbeschluss verkenne aufgrund der Rechtslage in den USA noch immer die Anforderungen des EuGH aus der Schrems-Rechtsprechung und verletze daher Art. 7, 8 und 47 der GRCh sowie Art. 22 und 45 der DSGVO.

a. Rechtliche Würdigung des EuG

Das EuG zeigt sich in seinem Urteil von den Anpassungen im US-Recht überzeugt. Insbesondere die Beschränkung der Überwachungsmaßnahmen auf das erforderliche und verhältnismäßige Maß sowie die Möglichkeit einer gerichtlichen ex-post-Kontrolle führen nach Ansicht der Richter zu einer Vereinbarkeit mit dem Datenschutzgrundrecht aus Art. 7 und 8 GRCh. Auch der Rechtsschutzmechanismus sei mit Art. 47 GRCh und den Grundsätzen der Schrems-Rechtsprechung vereinbar.

Zwar handele es sich bei dem DPRC nicht um ein Gericht im engeren Sinne des Art. 47 GRCh, da es nicht Teil der Judikative, sondern der Exekutive ist und auch nicht durch ein Parlamentsgesetz, sondern durch Verwaltungsvorschrift eingesetzt wurde. Jedoch formuliert der EuGH in Schrems II selbst, dass es sich um ein „Organ“ handeln müsse, und verwendet nicht den engeren Begriff des Gerichts.[11] Des Weiteren verlange ein Angemessenheitsbeschluss lediglich, dass der Rechtsschutz in der Sache gleichwertig, nicht jedoch in jeder Hinsicht identisch sein muss. Ein ausreichend unabhängiges Verwaltungsgremium könne diese Voraussetzungen daher erfüllen, sofern es in der Sache effektiven Rechtsschutz gewährleistet. Eben dies sieht das Gericht durch die Zusicherungen bezüglich der Unabhängigkeit von PCLOB, CLPO und DPRC in den US-Verwaltungsvorschriften als erfüllt an.

b. Kritischer Ausblick

Das Urteil des EuG erscheint mit Blick auf die eher strenge und eindeutige Rechtsprechung des EuGH in Sachen Schrems I und II überraschend. Die Neufassung des Wordings in der Executive Order 14086 bezüglich der Überwachungsmaßnahmen („Erforderlichkeit und Verhältnismäßigkeit“) ist erkennbar an den EU-Grundrechtsduktus angelehnt (zuvor as tailored as feasible).[12] Das EuG gibt sich mit dieser Umetikettierung zufrieden. Entscheidend für die Grundrechtskonformität mit Art. 7 und 8 der GRCh ist aber gerade nicht die Benennung der Rechtsbegriffe, sondern deren Auslegung - was das EuG gutmütig verkennt. Ob sich die Praxis der Überwachungsmaßnahmen dadurch tatsächlich geändert hat, wird nicht geprüft. Auch die rechtliche Würdigung des Rechtsschutzmechanismus wirft mehr Fragen auf, als sie beantwortet. Zwar rekurriert das EuG auf die zahlreichen Vorgaben im US-Recht zur Unabhängigkeit der jeweiligen Gremien (PCLOB, CLPO und DPRC), lässt dabei aber aktuelle Entwicklungen in den USA außer Betracht. So hat US-Präsident Trump bereits im Januar 2025 drei von den Demokraten ernannte Mitglieder des PCLOB entlassen.[13] Das Gremium, das die Arbeit des DPRC und des CLPO überwacht und als einziges öffentliche Informationen hierüber bereitstellt, besteht seitdem lediglich aus einer einzigen Person - die von den Republikanern ernannte Beth Williams.[14]

10 Mitglied der französischen Nationalversammlung für die liberale Mouvement démocrate.

11 EuGH, Urteil vom 16. Juli 2020, Schrems II, Rs. C 311/18, Rn. 197 (ECLI:EU:C:2020:559).

12 EuGH, Urteil vom 16. Juli 2020, Schrems II, Rs. C 311/18, Rn. 64 (ECLI:EU:C:2020:559).

13 https://www.nytimes.com/2025/01/22/us/trump-privacy-civil-liberties-oversight-board.html.

14 https://www.pclob.gov/Board/Index.

Aber auch ohne diese jüngeren Entwicklungen in den Blick zu nehmen, erscheint die unkritische Prüfung durch das EuG bemerkenswert. Denn bislang hat sich wohl der DPRC mit keiner einzigen Beschwerde eines Betroffenen befasst.[15] Das kann entweder bedeuten, dass die Überwachungsmaßnahmen in den USA völlig rechtskonform sind, und EU-Bürger daher keine Verfahren anstreben, oder aber, dass der Rechtsschutzmechanismus derart ineffektiv ist, dass die Beschwerdeführer ihn deswegen nicht in Anspruch nehmen. Dieser Prüfung entzieht sich das EuG jedoch und beurteilt vielmehr auf formeller Ebene die Konformität des CLPO und des DPRP mit den Rechtsschutzanforderungen nach Art. 47 GRCh.

Ob diese Bewertung der Berufung durch den EuGH standhalten wird, ist daher durchaus fraglich.

15 So einer der ehemaligen Special Advocates vor dem DPRC, Paul Rosenzweig https://www.nytimes.com/2025/01/22/us/trump-privacy-civil-liberties-oversight-board.html.

Impressum

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: dfn-verein@dfn.de

Texte:

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der Universität Münster und der Humboldt-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

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

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

Tel. (030) 838-66754

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