„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

6 / 2026
Juni 2026

Cookie-Einwilligungsbanner, quo vadis?

Ein Beitrag über die neuesten Entwicklungen zu Cookie- Einwilligungsbannern und Einwilligungsverwaltungsdiensten

Generative KI in der Forschung: Umbruch ohne Regeln?

Generative KI ist in der Forschung angekommen - die Regeln dazu noch nicht

Happy Birthday Datenschutz-Folgenabschätzung

In der Datenschutz-Grundverordnung (DSGVO) wurde im Jahr 2016 erstmals die Datenschutz-Folgenabschätzung (DSFA) auf europäischer Ebene kodifiziert

Kurzbeitrag: Durchgefallen

Thüringer Oberlandesgericht (OLG) erklärt Proctoring der Universität Erfurt für datenschutzwidrig

Cookie-Einwilligungsbanner, quo vadis?

Ein Beitrag über die neuesten Entwicklungen zu Cookie- Einwilligungsbannern und Einwilligungsverwaltungsdiensten

Von Anna Maria Yang-Jacobi

Cookie-Einwilligungsbanner auf Websites beschäftigen Aufsichtsbehörden, Gerichte und vor allem auch Internetnutzer:innen schon seit Jahren. Während sich einerseits immer deutlichere Vorgaben zur rechtskonformen Gestaltung herauskristallisieren, prüfen Gesetzgeber andererseits Möglichkeiten, der „Cookie-Banner-Flut" endlich ein Ende zu setzen. So nahm der erste anerkannte Dienst zur Einwilligungsverwaltung Anfang 2026 seine Arbeit auf. In der Zwischenzeit hat sich auch die EU-Kommission in ihrem Entwurf zu einer Digital-Omnibus-Verordnung[1] mit Änderungen der Cookie-Regelungen befasst. Das gibt Anlass, sich mit den rechtlichen Hintergründen zu Cookies und Datenverarbeitungen auf Websites zu beschäftigen. Denn auch Websites von Hochschulen sind von diesen Entwicklungen betroffen.

I. Verschiedene „Arten" der Einwilligung beim Website-Besuch

Besucher:innen von Websites kennen sie nur allzu gut: Cookie-Einwilligungsbanner, die regelmäßig auftauchen, bevor der eigentliche Inhalt der Website sichtbar ist. Cookies sind Textdateien, die Websites über den jeweiligen Internetbrowser speichern und auf den Endgeräten der Nutzer:innen ablegen.[2] Mithilfe dieser Dateien können die Betreiber der Website Nutzer:innen während des Website-Aufenthalts tracken oder bei einem erneuten Besuch der Website wiedererkennen. Je nach Speicherdauer unterscheidet man zwei Arten von Cookies: Sogenannte „Session-Cookies" speichern Informationen nur im Rahmen der jeweiligen Sitzung (engl. Session), während „permanente" Cookies Informationen über eine Session hinaus speichern. Cookies können zwar technisch notwendig sein, etwa um das ordnungsgemäße Funktionieren der Website sicherzustellen. Ist dies jedoch nicht der Fall, müssen die Nutzer:innen dem Einsatz von Cookies zustimmen.

1. Bestimmungen des TDDDG

Bereits 2002 enthielt die sogenannte ePrivacy-Richtlinie (RL)[3] Regelungen, um den Schutz der Privatsphäre und der Integrität informationstechnischer Geräte und Systeme zu gewährleisten. Die Cookie-Regelung in Art. 5 Abs. 3 ePrivacy-RL war damals jedoch noch so ausgestaltet, dass Nutzer:innen die Datenspeicherung aktiv verweigern mussten. Taten sie dies nicht, fand die Datenspeicherung statt. 2009 passte der europäische Gesetzgeber diese Regelung an: Das „Opt-out" wurde zu einer „Opt-in"-Lösung. So ist seitdem in der Regel eine Einwilligung der Website-Besucher:innen für die Informationsspeicherung durch Cookies erforderlich.

---

1 EU-Kommission, COM (2025) 837 final, 19.11.2025, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52025PC0837 (Alle Links dieses Beitrags wurden zuletzt am 20.04.2026 abgerufen).
Die Digital-Omnibus-Verordnung zielt darauf ab, einige europäische Digitalrechtsakte anzupassen, um die Innovationskraft und Wettbewerbsfähigkeit Europas zu stärken. Siehe zu den geplanten Änderungen der DSGVO: Müller-Westphal, Alles bleibt anders, DFN-Infobrief Recht 2/2026.

2 Allgemein zu Cookies siehe John, Ein Tool, die Banner zu knechten, DFN-Infobrief Recht 01/2022 und Baur, Noch viel zu knabbern, DFN-Infobrief Recht 05/2021.

3 RL 2002/58/EG - Datenschutzrichtlinie für elektronische Kommunikation.

Die erforderliche Umsetzung dieser Regelung in das deutsche Recht ließ einige Zeit auf sich warten. Zunächst erfolgte sie mittels bereits bestehender Gesetze. Erst seit dem Inkrafttreten des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG)[4] im Jahr 2021 enthält das deutsche Recht mit § 25 eine eigene Regelung zum Umgang mit Cookies. Sie unterscheidet zwischen zwei „Arten" von Cookies: Solchen, in deren Verwendung Nutzer:innen einwilligen müssen, und solchen, die keiner Einwilligung bedürfen. § 25 Abs. 1 TDDDG legt dabei fest, dass Nutzer:innen grundsätzlich in die Verwendung von Cookies einwilligen müssen. In Deutschland ist diese Regelung also der Grund für die allgegenwärtigen Cookie-Einwilligungsbanner. In bestimmten Fällen befreit allerdings § 25 Abs. 2 TDDDG die Diensteanbieter davon, eine Einwilligung einzuholen. Für Websites ist regelmäßig § 25 Abs. 2 Nr. 2 TDDDG einschlägig. Nach § 25 Abs. 2 Nr. 2 TDDDG ist eine Einwilligung der Nutzer:innen nicht erforderlich, wenn die Cookies technisch unbedingt erforderlich sind, um einen digitalen Dienst zur Verfügung zu stellen. Setzen Website-Betreiber nur solche technisch unbedingt erforderlichen Cookies, müssen sie also keinen Cookie-Einwilligungsbanner einbinden.

2. Und was ist mit der DSGVO?

Ziel der 2016 verabschiedeten Datenschutz-Grundverordnung (DSGVO)[5] war es vor allem, datenschutzrechtliche Einheitlichkeit herzustellen. Auch Website-Betreiber:innen, die beispielsweise über ein Kontaktformular personenbezogene Daten erheben, müssen ihre Nutzer:innen seit Inkrafttreten der DSGVO im Mai 2018 durch eine Datenschutzerklärung i. S. d. Art. 13, 14 DSGVO über die Datenverarbeitung informieren. Zusätzlich verweist das TDDDG an bestimmten Stellen auch auf DSGVO-Begriffe, sodass diese bei seiner Anwendung heranzuziehen sind.

Es gibt jedoch auch andere Situationen, die theoretisch sowohl von der DSGVO als auch von der ePrivacy-RL bzw. der nationalen Umsetzung in Form des TDDDG erfasst sein können. Ein Beispiel dafür sind Cookies, die das Verhalten von Nutzer:innen nachverfolgen und in diesem Zusammenhang personenbezogene Daten verarbeiten. In solchen Fällen regelt Art. 95 DSGVO das Verhältnis der DSGVO zur ePrivacy-RL. Für Website-Betreiber:innen bedeutet die Regelung Folgendes: Sofern personenbezogene Daten in Verbindung mit der Website verarbeitet werden und darüber hinaus auch die Zielsetzung der sich überschneidenden Regelungen aus der ePrivacy-RL und der DSGVO übereinstimmt, sind die Pflichten aus der ePrivacy-RL vorrangig anwendbar. Bei einer Verarbeitung personenbezogener Daten in Form des Speicherns und Auslesens von Informationen in Endeinrichtungen ist dies für § 25 TDDDG als nationale Umsetzung des Art. 5 Abs. 3 ePrivacy-RL zu bejahen. So gelten die Bestimmungen des § 25 TDDDG vorrangig vor den Rechtsgrundlagen der DSGVO zur rechtmäßigen Verarbeitung personenbezogener Daten. Sollten personenbezogene Daten jedoch in einem späteren Schritt verarbeitet werden, liegt diese Verarbeitung nicht mehr im Anwendungsbereich des § 25 TDDDG und es sind wiederum die Vorgaben der DSGVO zu beachten.

3. Wann ist welche Bestimmung des TDDDG und/oder der DSGVO anzuwenden?

Erstens könnte ein Website-Betreiber Cookies setzen, die technisch mehr als erforderlich sind. In diesem Fall ist für die Speicherung von Informationen zunächst eine Einwilligung gemäß § 25 Abs. 1 TDDDG notwendig. Sofern unter den Informationen auch personenbezogene Daten sind, die in einem späteren Schritt verarbeitet werden, handelt es sich gerade auch um eine Verarbeitung i. S. d. Art. 4 Nr. 2 DSGVO. Dies ist etwa dann der Fall, wenn Betreiber einer Website das Surfverhalten ihrer Besucher:innen tracken sowie deren IP-Adressen speichern, um diese später zu analysieren[6] oder Dritt-Anbieter-Cookies[7] für die Einbettung von Karten, Videos oder Social-Media-Inhalten setzen, die Nutzer:innen über mehrere Websites hinweg verfolgen. Für

4 Zur Umbenennung von TTDSG zu TDDDG siehe Yang-Jacobi, Telemedien out, Digitale Dienste in!, DFN-Infobrief Recht 08/2024. Zu den anderen Regelungen des Gesetzes siehe John, TTDSG – Die Profis in spe, DFN-Infobrief Recht 05/2021.

5 Verordnung (EU) 2016/679.

6 Die BfDI ordnet das beliebte Analysetool Matomo beispielsweise in der Regel als einwilligungsbedürftig nach § 25 Abs. 1 TDDDG ein, wobei die IP-Adresse nur pseudonymisiert und nicht anonymisiert wird, sodass die DSGVO anwendbar ist, siehe https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telemedien/Matomo.html.

7 Es gibt eine weitere Unterscheidung zwischen sogenannten First-Party- bzw. Third-Party-Cookies. First-Party-Cookies werden von den Website-Betreibern selbst gesetzt, während Third-Party-Cookies von Dritten gesetzt werden (beispielsweise großen Big Tech-Unternehmen). Siehe zu dieser Unterscheidung Yang-Jacobi, Automatisierte Kontrollen als Gamechanger?, DFN-Infobrief Recht 07/2025.

die anschließende Datenverarbeitung nach der DSGVO braucht es dann zusätzlich eine Rechtsgrundlage der DSGVO, etwa eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO. Die Einwilligungen nach DSGVO und TDDDG können auch gebündelt werden, sofern die Nutzer:innen über alle Zwecke informiert werden und deutlich ist, dass mehrere Einwilligungen erteilt werden.

Zweitens könnten die Cookies jedoch technisch unbedingt erforderlich sein, aber dennoch nachfolgend personenbezogene Daten verarbeiten. Generell gilt bei § 25 Abs. 2 Nr. 2 TDDDG: Der Website-Betreiber muss die technische Notwendigkeit der Cookies prüfen und nachweisen können. Wenn die Cookies technisch unbedingt erforderlich sind, ist keine Einwilligung der Nutzer:innen in die Speicherung von Informationen auf dem Endgerät erforderlich. Für die anschließende rechtmäßige Verarbeitung personenbezogener Daten wird jedoch eine Rechtsgrundlage der DSGVO benötigt. Handelt es sich etwa um Session-Cookies, die Nutzereingaben beim Ausfüllen von Online-Formularen speichern oder Login-Informationen speichern, kommt für die weitere Datenverarbeitung als Rechtsgrundlage Art. 6 Abs. 1 lit. a bis lit. f DSGVO in Betracht. Website-Betreiber stützen sich oftmals mit dem Argument der Nutzungsfreundlichkeit auf eine Datenverarbeitung aus berechtigtem Interesse i. S. d. Art. 6 Abs. 1 lit. f DSGVO. Hochschulen könnten außerdem auch Art. 6 Abs. 1 lit. e DSGVO i. V. m. Landeshochschulgesetzen[8] als Daten verarbeitende Rechtsgrundlagen angeben. Denn der Betrieb einer Website und die damit einhergehende Information der Öffentlichkeit gehören zur Aufgabenerfüllung einer Hochschule. Das gilt beispielsweise gerade auch für Warenkorb-Cookies, die eine Universität in ihrem Onlineshop nutzt, damit ausgewählte Artikel bis zum Ende der Bestellung im Warenkorb gespeichert bleiben.

Drittens könnte ein Website-Betreiber mehr als technisch unbedingt erforderliche Cookies setzen, aber anschließend keine personenbezogenen Daten verarbeiten. Das ist beispielsweise der Fall, wenn Tracking-Cookies oder statistische Cookies, Daten wie die IP-Adresse nur anonym erfassen und auswerten. Für die Anwendung der Cookie-Bestimmungen nach § 25 TDDDG ist es unerheblich, ob im Anschluss personenbezogene Daten verarbeitet werden. Immerhin schützt § 25 TDDDG die Integrität des informationstechnischen Systems oder Geräts vor einem unbefugten Zugriff. Eine Einwilligung nach § 25 Abs. 1 S. 1 TDDDG muss also auch in diesem Fall eingeholt werden. Eine Rechtsgrundlage der DSGVO wird dagegen mangels Verarbeitung personenbezogener Daten nicht benötigt.

Viertens und letztens könnten Website-Betreiber nur technisch unbedingt erforderliche Cookies setzen und anschließend keine personenbezogenen Daten verarbeiten. Zu denken ist dabei an Cookies zu Sicherheits- und Betrugspräventionszwecken oder Cookies, die die Spracheinstellung einer Website verwalten. Hier bedarf es weder einer Einwilligung nach § 25 Abs. 2 Nr. 2 TDDDG, noch einer Rechtsgrundlage der DSGVO.

4. Was ist bei der Einwilligung zu beachten?

Sofern eine Website mehr als technisch unbedingt erforderliche Cookies enthält, müssen Nutzer:innen also gemäß § 25 Abs. 1 S. 1 TDDDG darüber informiert werden und aufgrund klarer und umfassender Informationen einwilligen. Gemäß § 25 Abs. 1 S. 2 TDDDG haben die Information und die Einwilligung der Nutzenden nach den Vorschriften der DSGVO zu erfolgen.[9] Art. 4 Nr. 11 DSGVO regelt, dass eine Einwilligung „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung […]“ ist. Weitere Bedingungen für die Einwilligung sind sodann in Art. 7 und 8 DSGVO zu finden.

Die Rechtsprechung hat die Voraussetzung an eine wirksame Einwilligung bei Cookies konkretisiert. In seinem „Planet 49“-Urteil[10] machte der Europäische Gerichtshof (EuGH) bereits 2019 deutlich, dass der Nutzende durch eine eindeutige bestätigende Handlung einwilligen muss[11] und zumindest die Funktionsdauer und potenzielle Empfänger der in den Cookies enthaltenen Informationen anzugeben sind.[12] Zur genauen Gestaltung der

8 In Berlin beispielsweise i. V. m. §§ 4, 6 Berliner Hochschulgesetz.

9 Zumindest sofern diese Anwendung findet, Assion, TTDSG § 25 Rn. 25.

10 EuGH, Urt. v. 1.10.2019 – C-673/17 – Planet 49. Zu diesem Urteil ausführlich Baur, Noch viel zu knabbern, DFN-Infobrief Recht 12/2019.

11 EuGH, Urt. v. 1.10.2019 – C-673/17, Planet 49, Rn. 61, 62.

12 EuGH, Urt. v. 1.10.2019 – C-673/17, Planet 49, Rn. 75-81.

Cookie-Einwilligungsbanner äußerten sich in den darauffolgenden Jahren vor allem die Datenschutzbehörden gemeinsam über die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK).[13] So besteht grundsätzlich Spielraum, wie ein Einwilligungsbanner in Sachen Farbe, Größe und Kontraste aussehen kann. Eine unterschiedliche Farbe der Einwilligungs- oder Ablehnungskästchen sorgt also nicht sofort für eine unwirksame Einwilligung. Die Optionen müssen allerdings jeweils lesbar sein und die Nutzer:innen müssen in der Lage sein, ihre Optionen auf einen Blick zu erkennen. Lediglich unzulässige Verhaltenssteuerungen (engl. Nudging), die auch innerhalb der DSGVO die Voraussetzungen einer wirksamen Einwilligung i. S. v. Art. 4 Nr. 11, Art. 7 DSGVO nicht mehr erfüllen, sind nicht erlaubt. Die DSK fordert wiederum eine Reihe an Informationen, die ohne Umschweife, also auf der ersten sichtbaren Ebene eines Cookie-Banners, sichtbar sein müssen. Darunter fallen Informationen wie der konkrete Zweck der Verarbeitung, ob Profile erstellt werden oder Daten auch außerhalb des EWR verarbeitet werden.[14] Weitere Informationen zu Cookies und Datenverarbeitungen können dagegen in der Datenschutzerklärung enthalten sein. Generell gilt allerdings: Es muss eine Widerrufsmöglichkeit für die Einwilligung bestehen, die genauso leicht vollzogen werden kann, wie die Erteilung der Einwilligung (Art. 7 Abs. 3 S. 4 DSGVO).

Im März 2025 befasste sich ein deutsches Gericht zuletzt tiefergehender mit der Gestaltung von Cookie-Bannern.[15] Ausgangspunkt des Urteils war eine Anordnung des niedersächsischen Landesdatenschutzbeauftragten gegen den Herausgeber des Online-Angebots einer lokalen Zeitung. Die Datenschutzbehörde bemängelte den Cookie-Banner auf der Website. Dieser ermögliche keine wirksame Einwilligung, da die Nutzer:innen durch die Gestaltung zu einer Einwilligung gezwungen werden, also die Einwilligung gerade nicht auf Freiwilligkeit und ausreichenden Informationen beruhe. Das Verwaltungsgericht (VG) Hannover gab der Datenschutzbehörde recht und stellte fest, dass die Nutzer:innen erstens nicht bereits auf der ersten Ebene und damit nicht hinreichend über alle Drittdienstleister und Datenverarbeitungen in Drittstaaten informiert wurden.[16] Zweitens machte das VG mit Verweis auf vergangene Rechtsprechung deutlich, dass ein Cookie-Banner jedenfalls „nicht so gestaltet sein [darf], dass es den Nutzer gezielt zur Abgabe der Einwilligung hinlenkt und von der Ablehnung der Cookies abhält".[17] Allerdings legte es nicht explizit fest, dass auf der ersten Ebene neben einer Möglichkeit im Sinne von „Alle akzeptieren" auch eine „Alle Ablehnen"-Option erforderlich sei. Auf der ersten Ebene müsse lediglich unmissverständlich auf die Wahlmöglichkeit hingewiesen werden.[18] Das VG Hannover schloss sich der bisherigen Rechtsprechung an: Es blieb den strengen Maßstäben zu irreführenden Banner-Gestaltungen treu, verdeutlichte aber auch die zulässigen Möglichkeiten der Gestaltung.

II. Endlich ein Ende der Cookie-Banner?

Gerade die Cookie-Einwilligungsbanner könnten jedoch ohnehin bald der Vergangenheit angehören. Seit einiger Zeit gibt es Überlegungen, wie der „Cookie-Banner-Flut" entgegengesteuert werden kann.

1. Nationale Lösung: Der „Consenter"

Bereits seit 2021 ist mit § 26 TDDDG das Konzept von Einwilligungsverwaltungsdiensten wie beispielsweise PIMS (engl.: Personal Information Management Systems/Services, kurz PIMS) in Deutschland gesetzlich verankert. PIMS sollen grundsätzlich ermöglichen, nur einmal Entscheidungen zu Cookies zu treffen. Die gespeicherten Einstellungen übermittelt das System dann an die jeweilige Website.[19] 2024 verabschiedete die Bundesregierung mit Zustimmung des Bundestags und Bundesrats auf Grundlage

13 Ausführlicher siehe DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste) Version 1.2, Stand November 2024, Rn. 127-137, https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf.

14 Ibid., Rn. 119 f.

15 VG Hannover, Urt. v. 19.3.2025 – 10 A 5385/22.

16 VG Hannover, Urt. v. 19.3.2025 – 10 A 5385/22, Rn. 84.

17 VG Hannover, Urt. v. 19.3.2025 – 10 A 5385/22, Rn. 86.

18 So gerade auch Weller, EuDIR 2025, 293, 301.

19 Zu den rechtlichen Rahmenbedingungen, wie PIMS ausgestaltet sein müssen, damit die Selbstbestimmung der betroffenen Personen gewahrt wird, siehe Stadler/Eickhoff/Schneider/Specht-Riemenschneider, ZD 2025, 609, 611.

des § 26 Abs. 2 TDDDG die Einwilligungsverwaltungsverordnung (EinwV),[20] die die Anforderungen an PIMS und Verfahren zur Anerkennung von PIMS sowie die technischen und organisatorischen Maßnahmen zur Integration festlegte.[21] Die EinwV ist zum 1. April 2025 in Kraft getreten. Ende 2025 erkannte die Bundesbeauftragte für den Datenschutz und Informationsfreiheit (BfDI) den ersten Dienst zur Einwilligungsverwaltung nach § 13 EinwV an.

Dieser Dienst mit dem Namen „Consenter" ist seit Anfang 2026 offiziell verfügbar. Nutzer:innen können sich den Consenter Einwilligungsagent herunterladen und als Plug-in in Browser wie Google Chrome, Firefox und Safari einfügen. Daraufhin ist es den Nutzer:innen überlassen, welchen Arten von Cookies sie zustimmen und welche sie ablehnen. Das Besondere ist: Consenter blockiert nicht sofort alle Arten von Cookie-Bannern. Viele Websites versuchen nämlich, datenschutzfreundlich zu sein und ihre Nutzer:innen über die Datenverarbeitungszwecke zu informieren. Ziel des Dienstes ist vielmehr, Nutzer:innen zu helfen, informierte Entscheidungen zu treffen. Zur Entscheidungshilfe gibt es zusätzlich kurze Erklärungen sowie Gründe für und gegen die Einwilligung. Sobald die Entscheidungen getroffen sind, kommuniziert Consenter im Idealfall automatisch mit allen über den Browser besuchten Websites und gibt die jeweilige Auswahl weiter. Consenter blockiert sodann nur Cookie-Banner, die die Entscheidung der Nutzer:innen nicht akzeptieren. Allerdings sind Websites nach der EinwV nicht dazu verpflichtet, die Vorgaben von Diensten wie Consenter zu übernehmen. Das Problem der „Cookie-Banner-Flut" wird so nicht abschließend gelöst. Nationale Lösungen sind in einem „World Wide Web" wenig zielführend.

2. Neuer europäischer Ansatz: Integration in DSGVO und europaweite Einführung von PIMS?

2025 legte die EU-Kommission die langersehnte ePrivacy-Verordnung, die endlich Klarheit schaffen sollte, nach vielen Jahren ad acta.[22] Sie blieb jedoch nicht untätig und widmete sich den Cookie-Bannern stattdessen an anderer Stelle. So stellte sie im Rahmen des Entwurfs einer Digital-Omnibus-Verordnung neue Pläne für den Umgang mit Cookie-Einwilligungsbannern vor.[23] Der darin vorgesehene Art. 88a Datenschutz-Grundverordnung-Entwurf (DSGVO-E) soll die Regelungen, die die Speicherung von oder den Zugriff auf personenbezogene Daten durch Cookies betreffen, in die DSGVO integrieren. Die Cookie-Vorgaben zu personenbezogenen Daten würden dann nicht mehr entsprechend einer ins nationale Recht umgesetzten Richtlinie, sondern als Teil einer Verordnung unmittelbar europaweit gelten.[24] Art. 5 Abs. 3 ePrivacy-RL würde somit zwar weiterhin die Pflicht der Mitgliedstaaten enthalten, die Speicherung von Informationen oder den Zugriff auf Informationen bei fehlender technischer Erforderlichkeit von einer Einwilligung der Nutzer:innen abhängig zu machen. Die EU-Kommission ergänzt Art. 5 Abs. 3 ePrivacy-RL in ihren Plänen jedoch zur Klarstellung dahingehend, dass die Regelung bei natürlichen Personen und personenbezogenen Daten keine Anwendung findet. Die alte Regelung würde in diesem Sinne nur noch auf nicht personenbezogene Daten Anwendung finden.

Der geplante Art. 88a Abs. 1 DSGVO-E sieht als Grundsatz auch die Einwilligung durch die Nutzer:innen vor. Nach Art. 88a Abs. 3 DSGVO-E ist eine Speicherung und anschließende Datenverarbeitung weiterhin nur rechtmäßig, wenn sie für einen von vier genannten Zwecken erforderlich ist. Neben den bereits aus § 25 Abs. 2 TDDDG bekannten Zwecken kommen zwei weitere hinzu: die Nutzungsanalyse des eigenen Dienstes zur eigenen Verwendung sowie ein Zugriff für Zwecke der IT-Sicherheit. Art. 88a Abs. 4 DSGVO-E sieht zudem genauere Vorgaben für die Einwilligung vor: Die Einwilligungsanfragen müssen mit einem einzigen Klick ablehnbar sein (lit. a), bei erfolgter Einwilligung für einen bestimmten Zeitraum darf keine neue Einwilligungsanfrage für denselben Zweck gestellt werden (lit. b) und bei der Ablehnung darf für mindestens sechs Monate keine weitere Einwilligungsanfrage für denselben Zweck gestellt werden (lit. c). Diese Änderungen wären allesamt Neuerungen zur bisherigen Praxis.

---

20 Verordnung über Dienste zur Einwilligungsverwaltung nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz vom 6.2.2025.

21 Ausführlich Schöbel, Ende der Cookie-Banner, DFN-Infobrief Recht 03/2025.

22 Siehe nur BfDI, ePrivacy-Verordnung: Das Ende einer langen Reise, https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telemedien/ePrivacy_Verordnung.html.

23 Dazu bereits Müller-Westphal, Alles bleibt anders, DFN-Infobrief Recht 2/2026.

24 Siehe auch Gebehenne/Siebler/Hennemann, EuDIR 2026, 10, 11.

Zusätzlich enthält der Entwurf auch eine Regelung zu Cookies, die die Arbeit von PIMS erleichtern könnte. Nach Art. 88b Abs. 1 DSGVO-E wären Website-Betreiber künftig dazu verpflichtet, ihre Online-Schnittstellen so zu gestalten, dass Nutzer:innen ihre Entscheidungen zur Einwilligung oder Ablehnung automatisiert übermitteln können. Dies soll gerade dafür sorgen, dass Website-Betreiber vermehrt mit PIMS zusammenarbeiten, die diese technischen Schnittstellen anbieten. Zudem sollen nach der EU-Kommission die Anbieter von Webbrowsern diejenigen sein, die die technischen Mittel zur Einwilligungsverwaltung der Nutzer:innen bereitstellen.

III. Ausblick

Noch in diesem Jahr gibt es hoffentlich erste Erkenntnisse zur Anwendung des „Consenter". Auch der Entwurf zur Digitalen Omnibus-Verordnung steht auf der europäischen Diskussionsagenda weit oben. Die Änderungsvorschläge haben im ersten Quartal 2026 bereits einige Stellungnahmen hervorgerufen. So sprachen sich beispielsweise der Europäische Datenschutzausschuss (EDSA, engl. EDPB) und der Europäische Datenschutzbeauftragte (EDSB, engl. EDPS) bezüglich der Integration der Cookie-Regelungen in der vorgeschlagenen Form eher kritisch aus,[25] begrüßten aber im Grundsatz die Vorschläge zu Online-Schnittstellen und PIMS.[26] Bis rechtsverbindliche Änderungen verabschiedet werden und in Kraft treten, wird es jedoch noch dauern.

Für Hochschulen und Forschungseinrichtungen gilt: Sofern nur technisch unbedingt erforderliche Cookies gesetzt werden, braucht es keinen Cookie-Einwilligungsbanner. Die technisch unbedingte Erforderlichkeit muss jedoch sorgfältig eingeordnet und nachgewiesen werden können. Außerdem ist aufmerksam zu prüfen, ob mehr als technisch erforderliche Cookies für die Website tatsächlich unbedingt notwendig sind. Falls ja, sollten die Cookie-Einwilligungsbanner möglichst datenschutzfreundlich gestaltet sein und die Nutzer:innen hinreichend informieren. Eine sorgfältige Auseinandersetzung mit dem Thema ist ratsam, denn die deutschen Datenschutzbehörden sind mittlerweile in der Lage, eine Vielzahl an Websites automatisiert zu kontrollieren.[27]

Außerdem sollten sich Hochschulen und Forschungseinrichtungen bereits frühzeitig mit Online-Schnittstellen zu Einwilligungsverwaltungsdiensten auseinandersetzen. Selbst wenn sich die bislang vorgesehenen Regelungen der Digital-Omnibus-Verordnung ändern sollten, bleiben § 26 TDDDG und die EinwV in Deutschland zunächst unverändert bestehen. Es lohnt sich also, sich mit diesen Diensten zu befassen und so womöglich einen kleinen Teil zur Eindämmung der „Cookie-Banner-Flut" beizutragen

25 EDPB-EDPS Joint Opinion 2/2026, 10.2.2026, Rn. 96 ff., https://www.edpb.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf.

26 Ibid., Rn. 108 ff.

27 Siehe ausführlich Yang-Jacobi, Automatisierte Kontrollen als Gamechanger, DFN-Infobrief Recht 7/2025.

Generative KI in der Forschung: Umbruch ohne Regeln?

Generative KI ist in der Forschung angekommen - die Regeln dazu noch nicht

von Dr. Paul Friedl

Von erfundenen Fußnoten bis zu vollautomatisierten Forschungsbots: Generative KI hält mittlerweile auch in Wissenschaft und Forschung Einzug. Was dabei rechtlich erlaubt ist, ist nicht immer klar. Wie reagieren Hochschulen auf die Entwicklungen und was müssen Forscher:innen beachten? Eine Annäherung.

I. Wie generative KI die Forschung verändert

Paul Erdős, geboren 1913 in Budapest, gilt als einer der wichtigsten Mathematiker des 20. Jahrhunderts. Zum umfangreichen Nachlass Erdős' gehört neben unzähligen Beiträgen zu Kombinatorik, Graphentheorie und Zahlentheorie auch eine lange Liste ungelöster mathematischer Probleme. Die Webseite „www.erdosproblems.com", die sich der Sammlung dieser Probleme widmet, zählt derzeit 1217 solcher Probleme. Am 6. Januar 2026 sprang der Zähler, der die Zahl der mittlerweile gelösten Erdős-Probleme angibt, von 472 auf 473. Problem Nr. 728, das von Erdős zuerst 1975 beschrieben wurde, gilt seitdem als gelöst. Das Besondere an dem Fall: Die Lösung des Problems wurde nicht von einem Menschen erdacht, sondern mehr oder weniger autonom von ChatGPT entworfen.[1]

Die Mathematik ist aber natürlich nicht das einzige akademische Feld, in dem generative KI derzeit massive Umbrüche auslöst. Auch Forscher:innen vieler anderer Disziplinen nutzen KI-Tools. Die Einbindung KI-gestützter Tools reicht dabei von ihrer Nutzung als Brainstorming-Partner, der bei der Ideengenerierung hilft, über den Einsatz als „wissenschaftlicher Mitarbeiter", der einschlägige Quellen zusammenfasst, bis hin zur Verwendung als Ghostwriter, der ausgehend von einer (potenziell auch äußerst rudimentären) Skizze einen vollständigen akademischen Beitrag verfasst. Forscher:innen der Informatik haben außerdem bereits sogenannte AI research agents eingesetzt, die vollautomatisiert Forschungsthesen entwickeln, Experimente durchführen und die Ergebnisse (erfolgreich)[2] bei prestigeträchtigen Konferenzen einreichen.

Wie in vielen anderen gesellschaftlichen Bereichen verbreiten sich auch in der Wissenschaft KI-Tools derzeit also überaus rasant. Weniger geklärt scheint hingegen, inwiefern ihre Verwendung rechtlich überhaupt zulässig ist. Darf KI im Forschungs- und Publikationsprozess unbeschränkt eingesetzt werden? Worauf müssen Forschende achten?

II. Forschungsrecht? Die Bedeutung von Hochschulordnungen

Es ist Teil der im Grundgesetz garantierten Forschungsfreiheit, dass der Staat keine umfassenden Vorgaben dazu macht, was wissenschaftliches Arbeiten ausmacht oder wie Wissenschaftler:innen in Deutschland zu forschen haben.

1 Für einen Überblick über den Fall siehe den folgenden Mastodon-Thread des berühmten Mathematikers Terence Tao, @Tao@Mathstodon.xyz, Post vom 07.01.2026, https://mathstodon.xyz/@tao/115855845720777387 (alle Links dieses Beitrags wurden zuletzt am 08.05.2026 abgerufen).

2 Ein Artikel des Forschungs-Agenten des japanischen Unternehmens sakana.ai bestand den Peer-Review-Prozess der Machine-Learning-Konferenz ICLR, die als eine der drei wichtigsten Konferenzen weltweit auf diesem Gebiet gilt, siehe sakana.ai, „The AI Scientist Generates its First Peer-Reviewed Scientific Publication", abrufbar unter: https://sakana.ai/ai-scientist-first-publication/.

Entsprechend existieren in Deutschland weder ein „Forschungsgesetz“ noch andere gesetzliche Regelwerke, die inhaltliche Vorgaben für die wissenschaftliche Tätigkeit oder den Einsatz von KI in der Forschung festlegen.

Dennoch ist auch wissenschaftliches Arbeiten kein rechtsfreier Raum. Eine vergleichsweise unmittelbare Regulierung erfolgt etwa über die Voraussetzungen und Anforderungen an wissenschaftliche Qualifikationen, beispielsweise im Rahmen von Promotion oder Habilitation. Auf diesem Weg werden Mindeststandards definiert, die zur Erreichung bestimmter akademischer Grade erfüllt werden müssen, gleichzeitig aber auch darüber hinaus die wissenschaftliche Praxis beeinflussen.

Voraussetzungen und Anforderungen an solche Qualifikationsarbeiten sind in Deutschland weder auf Bundes- noch auf Landesebene zentral geregelt. Nach den jeweiligen Landeshochschulgesetzen[3] sind vielmehr die Universitäten selbst dafür zuständig, die Voraussetzungen und Anforderungen an wissenschaftliche Qualifikationen in ihren Hochschulordnungen selbstständig festzulegen. An den Universitäten wird diese Aufgabe gewöhnlich von den jeweiligen Fakultäten übernommen. Sie bestimmen in Studien-, Promotions- und Habilitationsordnungen, wann eine Arbeit eine hinreichende Prüfungsleistung darstellt, etwa konkret zur Verleihung des Doktortitels qualifiziert.

III. Die Regel: Graubereiche statt klarer Grenzen

Bisher treffen viele Hochschulordnungen allerdings keine spezifischen Regelungen zum Einsatz von KI. Das wirft die Frage auf, ob auch unter anderen bestehenden Qualitätsanforderungen der Einsatz von KI-Tools Probleme bereiten kann. Promotionen an der Juristischen Fakultät der Ludwig-Maximilians-Universität München müssen beispielsweise „eine Versicherung an Eides statt über die Eigenständigkeit der erbrachten wissenschaftlichen Leistungen” enthalten.[4] Weiter muss es sich bei der Dissertation um eine „vertiefte, selbstständige wissenschaftliche Leistung der Doktorandin oder des Doktoranden” handeln.[5] Nicht bestanden ist die Promotion, wenn es sich um „eine an erheblichen Mängeln leidende, insgesamt nicht mehr brauchbare Leistung” handelt.[6] Außerdem kann das Promotionsvorhaben zu jedem Zeitpunkt eingestellt werden, wenn sich herausstellt, dass der oder die Doktorand:in im Promotionsverfahren „getäuscht” hat.[7]

Das wirft die Frage auf, ob bzw. wann der Einsatz von generativer KI ausschließt, dass es sich um eine „selbstständige” wissenschaftliche Leistung handelt oder aber eine unzulässige „Täuschung” vorliegt. Auch weil die Münchener Fakultät insofern keine weiterführenden Leitfäden bereitstellt oder auf andere bestehende Handreichungen guter wissenschaftlicher Praxis verweist, bereitet die Beantwortung dieser Fragen freilich Probleme.

IV. Auf der Suche nach der guten wissenschaftlichen Praxis

Letztlich wird man zur Auslegung derart unbestimmter Begriffe deshalb oft darauf zurückgreifen müssen, ob der konkrete Einsatz eines KI-Tools einen (groben) Verstoß gegen anerkannte Regeln der guten wissenschaftlichen Praxis darstellt, wie sie von fast allen Universitäten auch in universitätsweiten Satzungen zur „Sicherung guter wissenschaftlicher Praxis“ festgehalten werden.[8] Auch das verspricht jedoch wenig Klarheit. Ob beispielsweise die Verwendung von KI-generierten Textpassagen gekennzeichnet werden muss, wird von verschiedenen Stimmen unterschiedlich beurteilt. Die „Empfehlung zur Sicherung der guten wissenschaftlichen Praxis beim Umgang mit Künstlicher Intelligenz” der Leibniz-Gemeinschaft bestimmt etwa, dass die

3 Siehe bspw. Art. 64 Bayerisches Hochschulgesetz, § 67 Hochschulgesetz NRW, § 35 Berliner Hochschulgesetz.

4 § 8 Abs. 1 Satz 2 Nr. 5 Promotionsordnung der Ludwig-Maximilians-Universität München für die Juristische Fakultät (PromO LMU) (2017).

5 § 10 Abs. 1 PromO LMU.

6 § 19 Abs. 1 Satz 1 PromO LMU.

7 § 23 PromO LMU.

8 Siehe bspw. Ludwig-Maximilians-Universität München, „Ordnung der Ludwig-Maximilians-Universität München zur Sicherung guter wissenschaftlicher Praxis vom 17. November 2023“; diese Satzungen dienen der Umsetzung des Kodex „Leitlinien zur Sicherung guter wissenschaftlicher Praxis“ der Deutschen Forschungsgemeinschaft (DFG). Um DFG-Fördermittel erhalten zu können, müssen Wissenschaftseinrichtungen die Leitlinien des DFG-Kodex rechtsverbindlich umgesetzt haben. Der DFG-Kodex verpflichtet Wissenschaftler:innen zwar zur Einhaltung der leges artis, verhält sich aber nicht explizit zur Verwendung von KI-Technologien.

Verwendung von KI-Tools „immer offengelegt werden" muss.[9] Eine solche Offenlegung müsse die „mit Hilfe von KI erstellten oder bearbeiteten Inhalte unter Angabe der genutzten Software inklusive Eigentümer [und] Version", aber auch eine „vollständige Dokumentation der verwendeten Prompts mit Datierung" umfassen.[10] Teilweise wird darüber hinaus vertreten, dass auch ein öffentlicher Link zum KI-erstellten Inhalt in das Literaturverzeichnis aufgenommen werden müsste[11] oder auch KI-Nutzung zum „Brainstorming" oder bei der „Generierung möglicher Argumente/Gegenargumente oder Forschungsperspektiven" transparent gemacht werden müsste.[12] Guidelines des European Research Area Forum sind hingegen der Ansicht, dass zumindest die Nutzung von KI als „basic author support tool" nicht kennzeichnungspflichtig sei.[13] Und auch wenn Handreichungen überwiegend die Offenlegung des Einsatzes von KI nahelegen, scheint sich dieses Vorgehen in der gelebten wissenschaftlichen Praxis bisher nicht durchgesetzt zu haben.

V. Die Ausnahme: Spezifische Vorgaben

Etwas leichter haben es Nachwuchsforscher:innen, wenn anwendbare Promotionsordnungen klare(re) Vorgaben zur Zulässigkeit und Kennzeichnung von KI-generierten Inhalten machen. So bestimmt etwa die Promotionsordnung der Juristischen Fakultät der Humboldt-Universität zu Berlin: „KI-generierte Texte sind unzulässig. Ausgenommen sind die Verwendung von KI-gestützten Programmen zur Rechtschreibkontrolle, Grammatikkontrolle und Zeichensetzungskontrolle".[14] Promovierende der Medizinischen Fakultät der Ruhr-Universität Bochum müssen in einer eidesstattlichen Erklärung vor Einreichung der Promotion angeben, ob sie generative KI eingesetzt haben, ob die Nutzung dieser Hilfsmittel von der betreuenden Person explizit gestattet wurde und, falls ja, „welche Programme, zu welchem Zweck und in welchem Umfang". Außerdem müssen „KI-generierte Inhalte kenntlich gemacht und im Methodenteil der Dissertation dargestellt" werden.[15]

Derartige Regeln stellen im Vergleich zu Qualifikationsordnungen, die überhaupt nichts zum Einsatz von KI sagen, natürlich einen Fortschritt dar. Gleichzeitig bleibt offen, wie realitätsnah – und wie sinnvoll – sie in einer Zeit sind, in der KI-Tools für viele Menschen zum Alltagswerkzeug geworden sind.

VI. Jenseits der Hochschulordnung: Weitere Regelgeber im Forschungsumfeld

Hochschul- und Qualifikationsordnungen sind nicht die einzigen Regelwerke, die den Einsatz von KI in Forschung und Wissenschaft (mittelbar) regulieren. Auch Publikationsorgane, etwa wissenschaftliche Verlage oder Fachzeitschriften, beeinflussen durch Redaktionsrichtlinien und andere Regularien, welche Vorgaben für den KI-Einsatz in der wissenschaftlichen Arbeit gelten. Auch hier ist das Bild alles andere als einheitlich: Wo manche Verlage überhaupt keine Regeln zur Verwendung von KI-Tools vorhalten,[16]

---

9 Leibniz Association. (2024). Empfehlung zur Sicherung der guten wissenschaftlichen Praxis beim Umgang mit Künstlicher Intelligenz. Zenodo. https://doi.org/10.5281/zenodo.14420893.

10 Leibniz Association. (2024). Empfehlung zur Sicherung der guten wissenschaftlichen Praxis beim Umgang mit Künstlicher Intelligenz, S. 4. Zenodo. https://doi.org/10.5281/zenodo.14420893.

11 Institut für Kulturwissenschaft der Humboldt-Universität zu Berlin, Studienfachberatung, „Handreichung zum Umgang mit KI in schriftlichen Arbeiten und bei Verwendung von audio/visuellen Medien" (12.06.2025).

12 Bergische Universität Wuppertal, Fachgruppe Katholische Theologie, „Handreichung zum Umgang mit generativer KI in schriftlichen Arbeiten" (03.02.2026).

13 European Commission, „Living guidelines on the responsible use of generative AI in research (2. version)" (April 2025), Fn. 21; die Guidelines definieren allerdings nicht, was eine Verwendung als „basic author support tool" umfasst. Als Abgrenzung wird nur negativ festgehalten, dass „interpreting data analysis, carrying out a literature review, identifying research gaps, formulating research aims, developing hypotheses, etc." darüber hinaus gehen „könnten".

14 § 7 Abs. 2 Nr. 2 PromO (13. Februar 2025).

15 Medizinische Fakultät der Ruhr-Universität, „Eigenständigkeitserklärung gemäß § 9 PromO (2016) und Erklärung zur Verwendung von künstlicher Intelligenz (KI)" (30.06.2025).

16 So etwa die juristischen Zeitschriften des Verlags C.H. Beck.

sehen andere recht spezifische Vorgaben vor, die den in Hochschulordnungen verwendeten Ansätzen oft ähneln.[17] Denkbar ist schließlich weiter, dass auch Forschungsfördereinrichtungen und Geldgeber durch ihre Verwendungsrichtlinien oder andere Regularien den Einsatz von KI regulieren. Die Deutsche Forschungsgemeinschaft hält in ihrem Leitfaden für die Erstellung von Förderanträgen fest, dass die Verwendung von generativen KI-Tools in „wissenschaftsadäquater Weise" offenzulegen sei.[18] Genauere Vorgaben sollen noch folgen.

VII. Wie wollen wir forschen?

Nicht zuletzt, weil viele Universitäten, Forschungsakteure und Verlage, wie dargestellt, bisher noch keine Regeln zum Einsatz von KI implementiert haben, ist davon auszugehen, dass sich das regulatorische Bild in den kommenden Jahren weiter verändern wird. Möglich scheint, dass Ansätze, die den Einsatz von KI großflächiger zulassen, sich in Zukunft dabei größerer Beliebtheit erfreuen könnten. Dies womöglich allein deswegen, da sich Verstöße gegen KI-Verbote (derzeit) ohnehin schlecht nachweisen lassen. Das lenkt den Blick auch auf ein anderes Thema: Gibt es Technologien, die bei der Durchsetzung existierender Regularien helfen können? KI-Wasserzeichen und KI-Detektoren sind hier vielleicht nur der Anfang.[19] Versionierungs-Tools, mit denen das Entstehen eines Textes von Anfang bis Ende nachverfolgt werden kann, könnten größere Zuverlässigkeit bringen.

Letztlich ist aber ohnehin unklar, ob es die rechtlichen Grenzen sind, die über die Zukunft der Wissenschaft im Zeitalter generativer KI entscheiden werden. Wahrscheinlicher - und wünschenswerter - scheint, dass darüber verschiedene Disziplinen und Forschungsgemeinschaften demokratisch unter sich entscheiden. Das wirft auch die Frage auf, was Sinn und Aufgabe unterschiedlicher wissenschaftlicher Disziplinen sind und was diese für den Einsatz generativer KI bedeuten. Auch dies sind große Fragen, die wir aufgrund ihrer Bedeutung in einem Folgebeitrag im nächsten Infobrief näher beleuchten wollen.

---

17 Die Richtlinie des internationalen Verlagshauses Wolters Kluwer bestimmt etwa, dass KI im Schreibprozess nur für die Verbesserung der Lesbarkeit und der Sprache benutzt werden darf und dass die Verwendung von KI nicht die eigenständige intellektuelle Anstrengung des*der Autor*in ersetzen darf, siehe Kluwer Law International B.V., „Publication Ethics and Malpractice Statement", abrufbar unter: https://kluwerlawonline.com/media/KLI_Publication_Ethics_Malpractice_Statement.pdf.

18 DFG, "Leitfaden für die Antragstellung Projektanträge", abrufbar unter: https://www.dfg.de/resource/blob/168312/54-01-de.pdf. Auf einer Webpage der DFG wird dies dahingehend präzisiert, dass „[u]nter „Offenlegung" […] aktuell die Angabe zu verstehen [ist], welche generativen Modelle zu welchem Zweck und in welchem Umfang eingesetzt wurden, beispielsweise bei der Aufbereitung des Forschungsstandes, bei der Entwicklung einer wissenschaftlichen Methode, bei der Auswertung von Daten oder bei der Hypothesengenerierung", siehe DFG, „KI in der Antragstellung", abrufbar unter: https://www.dfg.de/de/grundlagen-themen/digitale-themen/ki/antragstellung.

19 Siehe dazu auch den Beitrag im Infobrief Mai/2026, Friedl, „Mit KI-Wasserzeichen zu klareren Informationsökosystemen".

Happy Birthday Datenschutz-Folgenabschätzung

In der Datenschutz-Grundverordnung (DSGVO) wurde im Jahr 2016 erstmals die Datenschutz-Folgenabschätzung (DSFA) auf europäischer Ebene kodifiziert

Von Philipp Schöbel

In der DSGVO wurden mehrere neue Instrumente in das europäische Datenschutzrecht integriert. Zu diesen Instrumenten zählt auch die DSFA. Der Europäische Datenschutzausschuss (EDSA) hat im April ein vorläufiges Muster für die Durchführung der DSFA veröffentlicht.[1] Das Muster soll die Datenschutz-Compliance in Europa vereinfachen und zu einer harmonisierten Anwendung der DSGVO beitragen.[2] Für Hochschulen können die Anforderungen der DSFA insbesondere bei der Einführung von KI in Lehre und Verwaltung relevant sein.

I. Historische Entwicklung

Die DSFA gab es vor der Verabschiedung der DSGVO noch nicht. Zwar wurde bereits in der europäischen Datenschutzrichtlinie (DSRL)[3] der sogenannte risikobasierte Ansatz verfolgt, das Instrument des Art. 35 DSGVO war aber ein Novum.[4] Vorher existierte die Pflicht zur sogenannten Vorabkontrolle (Art. 20 DSRL). Diese legte eine Pflicht zur Prüfung spezifischer Risiken fest, war aber wesentlich abstrakter ausgestaltet als die Pflicht zur DSFA und wird in der Literatur nicht als konkrete Vorgängerregelung angesehen.[5]
Am 4. Mai 2016 wurde neben der DSGVO auch die Richtlinie zum Datenschutz in Strafsachen (JI-RL)[6] im Amtsblatt der Europäischen Union veröffentlicht. Diese enthält auch eine Pflicht zur DSFA (Art. 27 Abs. 1 JI-RL). Die Vorschrift aus der JI-RL ist in Deutschland in § 67 des Bundesdatenschutzgesetzes (BDSG) umgesetzt worden. Für Hochschulen und Forschungseinrichtungen dürfte die DSFA aus der DSGVO jedoch wesentlich relevanter sein.

II. Sinn und Zweck

Die Durchführung einer DSFA dient der Ermittlung der mit der Datenverarbeitung verbundenen Risiken.[7] Schon im Vorfeld

1 EDSA, EDPB DPIA Template, 14.04.2026, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template_en (alle Quellen zuletzt abgerufen am 06.05.2026).

2 Vgl. EDSA, Enhancing compliance and consistency: EDPB adopts DPIA template, 14.04.2026, abrufbar unter: https://www.edpb.europa.eu/news/news/2026/enhancing-compliance-and-consistency-edpb-adopts-dpia-template_de.

3 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 S. 31.

4 Martini, in: Paal/Pauly, 4. Aufl. 2026, VO (EU) 2016/679 Art. 35 Rn. 12.

5 Hansen, in: BeckOK DatenschutzR, 55. Ed. 1.2.2024, DS-GVO Art. 35 Rn. 1.

6 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.

7 Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 3. Auflage 2025, S. 292, Rn. 42-43.

der Datenverarbeitung sollen so mögliche Schwachstellen und Gefährdungsgrade aufgezeigt werden.[8] Sie stellt daher eine Art „Frühwarnmechanismus“ dar.[9] Betrachtet werden sollen dabei sowohl die Auswirkungen der rechtlichen als auch der technischen Risiken der Datenverarbeitung auf die Rechte der betroffenen Personen.[10]

III. Adressat:innen der Pflicht

Der/die Verantwortliche ist verpflichtet, die DSFA durchzuführen (Art. 35 Abs. 1 DSGVO).[11] Die Pflicht trifft nicht die Datenschutzbeauftragten.[12] Der/die Verantwortliche holt aber den Rat der/des Datenschutzbeauftragten ein (Art. 35 Abs. 2 DSGVO). Ebenfalls nicht Adressat:in der Norm ist der/die Auftragsverarbeiter:in, auch wenn diese den/die Verantwortliche(n) bei der DSFA unterstützen müssen (Art. 28 Abs. 2 S. 3 lit. f DSGVO).[13] Der EDSA empfiehlt, dass der/die Verantwortliche schriftlich dokumentiert, welche Organisationseinheit für die Datenverarbeitung intern verantwortlich ist.[14] Auch sollten Informationen zu der/dem Datenschutzbeauftragten und den Auftragsverarbeiter:innen festgehalten werden.

IV. Voraussetzungen

Die DSFA muss vor der Inbetriebnahme der Datenverarbeitung durchgeführt werden.[15] Dementsprechend sollten ihre Voraussetzungen auch vor dem Beginn der Verarbeitung geprüft werden. Der EDSA empfiehlt, das geplante Startdatum und die Bezeichnung der Verarbeitung zu dokumentieren.[16]

Eine DSFA muss durchgeführt werden, wenn eine Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (Art. 35 Abs. 1 S. 1 DSGVO). Dies gilt insbesondere bei der Verwendung neuer Technologien. Relevant ist dies etwa beim Einsatz von KI im Rahmen von Immatrikulation, Klausurenkorrektur oder Plagiatserkennung. Denn viele der unterschiedlichen KI-Anwendungen dürften zumindest derzeit noch neue Technologien darstellen. Gerade beim Einsatz von KI in der Lehre kann eine Prüfung der Voraussetzung der DSFA angezeigt sein.

1. Hohes Risiko

Ein Risiko im Sinne des Art. 35 DSGVO ist die Kombination aus der potenziellen Schwere eines Schadens und seiner Eintrittswahrscheinlichkeit.[17] Es gibt jedoch keine einheitliche Bewertungsskala, um zu ermitteln, wann ein Risiko als hoch einzustufen ist.[18]

2. Gesetzliche Regelfälle

Die DSGVO sieht drei Regelfälle vor, bei deren Vorliegen eine DSFA erforderlich ist. Der erste dieser drei Fälle ist die systematische und umfassende Bewertung persönlicher Aspekte von natürlichen Personen (Art. 35 Abs 3 lit. a DSGVO). Zu diesen Aspekten zählen etwa Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel.[19] Die Bewertung muss auf einer automatisierten Verarbeitung beruhen. Umfasst sind sowohl die

8 Martini, in: Paal/Pauly, 4. Aufl. 2026, VO (EU) 2016/679 Art. 35 Rn. 6.

9 Martini, in: Paal/Pauly, 4. Aufl. 2026, VO (EU) 2016/679 Art. 35 Rn. 6.

10 Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, 2. Aufl. 2025, DS-GVO Art. 35 Rn. 12.

11 Hansen, in: BeckOK DatenschutzR, 55. Ed. 1.2.2024, DS-GVO Art. 35 Rn. 10.

12 Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 3. Auflage 2025, S. 293, Rn. 46.

13 Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 3. Auflage 2025, S. 293, Rn. 48.

14 EDSA, EDPB DPIA Template, 14.04.2026, S. 4.

15 Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 3. Auflage 2025, S. 293, Rn. 50.

16 EDSA, EDPB DPIA Template, 14.04.2026, S. 4.

17 Martini: Paal/Pauly, 4. Aufl. 2026, VO (EU) 2016/679 Art. 35 Rn. 15a.

18 Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, 2. Aufl. 2025, DS-GVO Art. 35 Rn. 23 mwE.

19 Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, 2. Aufl. 2025, DS-GVO Art. 35 Rn. 47.

vollständig automatisierte als auch die teilweise automatisierte Verarbeitung.[20] Zudem muss diese Verarbeitung als Grundlage für eine Entscheidung dienen, die entweder eine Rechtswirkung gegenüber natürlichen Personen entfaltet oder sie in ähnlicher Weise beeinträchtigt. Relevante rechtliche Entscheidungen im Hochschulsektor können etwa die Imma- oder Exmatrikulation sowie die Bewertung einer Prüfungsleistung sein.

Der zweite Regelfall ist die umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 oder Art. 10 DSGVO. Daten nach Art. 9 Abs. 1 DSGVO sind zum einen solche, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen. Zum anderen sind es genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung. Daten nach Art. 10 DSGVO sind solche über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln. Auch hier sollte beim Einsatz von KI in Immatrikulations-/oder Studienbewerbungsverfahren geprüft werden, ob sensible Daten verarbeitet werden.

Den dritten Regelfall bildet die systematische, umfangreiche Überwachung öffentlich zugänglicher Bereiche (Art. 35 Abs. 3 lit. c DSGVO). Die Formulierung ist technologieneutral und erfasst nicht nur „klassische" Überwachung mittels Videotechnologie, sondern auch WLAN- und Bluetooth-Technologie sowie Gesichts- oder Emotionserkennung.[21] „Öffentlich zugänglicher Bereich" meint, dass der Zugang für eine unbestimmte Anzahl an Personen sowohl möglich als auch dafür bestimmt ist.[22] Gerade bei der Überwachung von Teilen eines Campus sollte geprüft werden, ob die entsprechenden Bereiche (etwa Mensa, Eingangsbereiche oder Schließfächer) öffentlich zugänglich sind. Zudem muss die Überwachung gerade systematisch und umfangreich sein. Eine systematische Überwachung kann etwa vorliegen, wenn sie vorab arrangiert, organisiert und methodisch durchgeführt wird.[23] „Umfangreich" kann sich sowohl aus der Größe des überwachten Bereichs als auch aus einer hohen Zahl überwachter Personen ergeben.[24]

V. Inhalt der Folgenabschätzung

Das Gesetz schreibt für den Inhalt der Folgenabschätzung nur einen Mindestkatalog vor (Art. 35 Abs. 7 DSGVO). Die dort vorgeschriebenen Inhalte werden allgemein in drei unterschiedliche Phasen eingeteilt: Vorbereitungsphase, Bewertungsphase und Maßnahmenphase.[25] In der Vorbereitungsphase müssen die geplanten Verarbeitungsvorgänge und Verarbeitungszwecke systematisch beschrieben werden (Art. 35 Abs. 7 lit. a DSGVO). Dort sind auch die verfolgten berechtigten Zwecke nach Art. 6 Abs 1 lit. f DSGVO zu beschreiben. Das Muster des EDSA sieht die Beschreibung der Kategorien von personenbezogenen Daten vor.[26] Auch soll an dieser Stelle bereits aufgeführt werden, ob es sich bei den verarbeiteten Daten um besonders sensible Daten im Sinne des Art. 9 Abs. 1 DSGVO handelt. Hinsichtlich der Verarbeitungszwecke empfiehlt der EDSA hier auch, sekundäre oder kompatible Verarbeitungszwecke aufzuführen. Darüber hinaus sollten Art, Umfang und Kontext der Verarbeitung nach dem Muster des EDSA an dieser Stelle beschrieben werden.[27] Die Art der Datenverarbeitung umfasst etwa die durchgeführten Vorgänge und eingesetzten Technologien. Beispiele für den Umfang sind etwa die Anzahl der betroffenen Personen, der geografische Erfassungsbereich sowie die Häufigkeit oder Dauer. Der Kontext der Verarbeitung meint unter anderem die Anwendungsfälle, Kategorien betroffener Personen inklusive potenziell schutzbedürftiger Gruppen, grenzüberschreitende Verarbeitungen sowie internationale Datenübermittlungen. Der EDSA empfiehlt die Rechtsgrundlagen für die Verarbeitung

20 Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, 2. Aufl. 2025, DS-GVO Art. 35 Rn. 46.

21 Martini: Paal/Pauly, 4. Aufl. 2026, VO (EU) 2016/679 Art. 35 Rn. 31.

22 Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, 2. Aufl. 2025, DS-GVO Art. 35 Rn. 52.

23 Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, 2. Aufl. 2025, DS-GVO Art. 35 Rn. 52.

24

25 Martini: Paal/Pauly, 4. Aufl. 2026, VO (EU) 2016/679 Art. 35 Rn. 44a.

26 EDSA, EDPB DPIA Template, 14.04.2026, S. 7.

27 EDSA, EDPB DPIA Template, 14.04.2026, S. 8.

aufzuführen und zwischen denen des Art. 6 Abs. 1 und denen des Art. 9 Abs. 2 DSGVO zu unterscheiden.[28] Auch sollen Maßnahmen zur Datenminimierung und Datenqualität beschrieben werden.[29] Darüber hinaus sieht der EDSA auch eine Beschreibung der DSGVO-Compliance-Maßnahmen vor.[30] Dazu gehören etwa Maßnahmen zur Einhaltung der Datenschutzgrundsätze (Art. 5 DSGVO), der Rechte der betroffenen Personen (Art. 12-22 DSGVO) oder zur Sicherheit der Verarbeitung (Art. 32 DSGVO).

Die Bewertungsphase umfasst eine Beurteilung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck sowie die Risiken für die Rechte und Freiheiten der betroffenen Personen (Art. 35 Abs. 7 lit. b, c DSGVO). Für die Bewertung der Notwendigkeit und Verhältnismäßigkeit schlägt der EDSA einen dreistufigen Aufbau vor.[31] In einem ersten Schritt werden die Auswirkungen der Datenverarbeitung in ihrer geplanten Durchführung auf die Rechte und Freiheiten der betroffenen Person beurteilt. Hier werden potenzielle Risiken der Verarbeitung beschrieben und wie sich diese verwirklichen können. An dieser Stelle werden auch die unterschiedlichen Gefahrenquellen (etwa schlechtes Design oder Schwachstellen) beschrieben. Danach werden Notwendigkeit und Verhältnismäßigkeit dargestellt. Daran schließt sich eine zweite Risikobewertung an.[32] Diese richtet sich aber nicht auf die Risiken der Verarbeitung in ihrer geplanten Durchführung. Vielmehr geht es um Risiken, die durch Fehler oder Abweichungen von der geplanten Datenverarbeitung entstehen (der EDSA geht davon aus, dass Notwendigkeit und Verhältnismäßigkeit sich nicht auf diese zweite Kategorie von Risiken beziehen). Der EDSA empfiehlt, dann die Risiken beider Kategorien (geplante Verarbeitung und Abweichungen von der geplanten Verarbeitung) gemeinsam zu bewerten. Hierfür soll die zu wählende Methode zunächst beschrieben werden: etwa unterschiedliche Wahrscheinlichkeitsgrade, unterschiedliche Grade der Risikopriorisierung und welche Grade von Risiken als hinnehmbar gelten. In der Risikobewertung soll dann unter anderem dargestellt werden, welche Wahrscheinlichkeit und welche Intensität den einzelnen Risiken zugeordnet werden. Auf dieser Grundlage soll dann aufgezeigt werden, ob die Risiken akzeptabel sind.

Die Maßnahmenphase enthält die geplanten Abhilfemaßnahmen, die der Risikobewältigung dienen (Art. 35 Abs. 7 lit. d DSGVO). Sie bildet den Schlussstein der DSFA. Der EDSA empfiehlt einen dreistufigen Aufbau der Maßnahmenphase.[33] Die erste Stufe bildet die Darstellung der Abhilfemaßnahmen. Zunächst sollen alle technischen, rechtlichen und organisatorischen Abhilfemaßnahmen aufgeführt werden. Den einzelnen Maßnahmen sollen die Risiken, die sie mindern sollen, zugeordnet werden. Anschließend sollen ihre Angemessenheit und Effektivität aufgeführt werden. Die zweite Stufe bildet die Beschreibung der verbleibenden Restrisiken. Sie ist eine erneute Risikobeurteilung unter Zugrundelegung der beschriebenen Risikomaßnahmen. Hier soll beurteilt werden, ob das Restrisiko akzeptabel ist oder nicht. Die dritte Stufe ist die Darstellung des Risikoplans. Dieser Plan soll aufzeigen, wie die Abhilfemaßnahmen in die Datenverarbeitung integriert werden. Zudem ist darzustellen, wie die Maßnahmen nach dem Beginn der Datenverarbeitung überwacht, überprüft und aktualisiert werden können. Hier sind etwa individuelle Verantwortlichkeiten innerhalb der Organisation sowie festgelegte Zeitpläne darzustellen.

Der EDSA empfiehlt, anschließend an die eigentliche DSFA auch den Rat der Datenschutzbeauftragten sowie den Standpunkt der betroffenen Personen zu dokumentieren. Als Letztes soll die getroffene Entscheidung dokumentiert werden.

VI. Fazit

Mit dem Aufkommen neuer Anwendungsfelder von KI in Lehre und Verwaltung wird die DSFA weiterhin relevant bleiben. Hochschulen und Forschungseinrichtungen stehen vor der Aufgabe, den Einsatz von KI datenschutzkonform umzusetzen. Wie sie die DSFA innerhalb des gesetzlichen Rahmens konkret durchführen,

28 EDSA, EDPB DPIA Template, 14.04.2026, S. 9.

29 EDSA, EDPB DPIA Template, 14.04.2026, S. 11.

30 EDSA, EDPB DPIA Template, 14.04.2026, S. 12 f.

31 EDSA, EDPB DPIA Template, 14.04.2026, S. 15.

32 EDSA, EDPB DPIA Template, 14.04.2026, S. 16.

33 EDSA, EDPB DPIA Template, 14.04.2026, S. 17.

ist allerdings ihnen überlassen. Ob das nun vorgeschlagene Muster des EDSA die DSFA für Datenverarbeitungen in Lehre und Hochschulverwaltung erleichtert, wird sich noch zeigen müssen.

DFN Infobrief-Recht-Aktuell

- ## EU-Recht/Digitale Identitäten: Referentenentwurf zum Digitale-Identitäten-Gesetz (DIdG)

  Das Bundesministerium für Digitales und Staatsmodernisierung hat am 26. März 2026 einen Referentenentwurf für ein Gesetz für digitale Identitäten veröffentlicht. Mit dem Gesetz sollen die Vorgaben zur Umsetzung der europäischen EUDI-Wallet in nationales Recht konkretisiert werden. Geplant ist, dass ab dem Jahr 2027 Bürger:innen mithilfe der sogenannten EUDI-Wallet Dokumente wie Personalausweis oder Führerschein auf dem Smartphone vorhalten und verwenden können. Der Entwurf regelt insbesondere die Zuständigkeit der beteiligten Behörden sowie die Bereitstellung und staatliche Aufsicht über die Wallet.

  Hier erhalten Sie den Link zum Referentenentwurf (alle Links dieser Seite wurden zuletzt am 28.05.2026 abgerufen):
  https://bmds.bund.de/fileadmin/BMDS/Dokumente/Gesetzesvorhaben/DIdG_RefE_26-03-2026-barrierefrei.pdf

- ## Verfassungsrecht/Hochschulrecht: Beschluss des Bundesverfassungsgerichts (BVerfG) zur Zweitveröffentlichungspflicht wissenschaftlichen Personals nach § 44 Abs. 6 des Gesetzes über die Hochschulen in Baden-Württemberg

  Das BVerfG hat mit Beschluss vom 24. März 2026 entschieden, dass § 44 Abs. 6 des Gesetzes über die Hochschulen in Baden-Württemberg mit Artikel 71 und Artikel 73 Abs. 1 Nr. 9 des Grundgesetzes unvereinbar und nichtig ist, da es sich um eine Regelung auf dem Gebiet des Urheberrechts im Sinne der ausschließlichen Gesetzgebungskompetenz des Bundes handelt.
  Hier erhalten Sie den Link zur Entscheidung::
  https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2026/03/ls20260324_2bvl000318.html

- ## Datenschutzrecht: Entscheidung des Bundesverwaltungsgerichts (BVerwG) zum Einsichtsrecht der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) in Unterlagen des Bundesnachrichtendienstes (BND)

  Das BVerwG hat mit Urteil vom 4. März 2026 die Klage der BfDI auf Gewährung von Einsichtsrecht in Unterlagen des BND als unzulässig abgewiesen. Der geltend gemachte Anspruch auf Einsichtnahme stützte sich auf § 63 BNDG i.V.m. § 28 Abs. 3 S. 2 Nr. 1 BVerfSchG. Nach Auffassung des Gerichts begründen diese Vorschriften keine durchsetzbare wehrfähige Rechtsposition der BfDI auf Einsichtnahme. Die vorhandenen Regelungen sehen vielmehr vor, dass bei Verweigerung der Einsichtnahme durch den BND die Maßnahme einer Beanstandung gegenüber dem Bundeskanzleramt möglich sei.
  Hier erhalten Sie den Link zur Pressemitteilung:
  https://www.bverwg.de/de/pm/2026/15

Kurzbeitrag: Durchgefallen

Thüringer Oberlandesgericht (OLG) erklärt Proctoring der Universität Erfurt für datenschutzwidrig

Von Nils Bielzer

KI-basiertes Proctoring[1] unter Nutzung biometrischer Daten verstößt laut Thüringer OLG ohne explizite Einwilligung gegen die Datenschutz-Grundverordnung (DSGVO). Ein Urteil vom 17. November 2025 (Az. 3 U 885/24)[2] setzt klare Grenzen für die digitale Prüfungsüberwachung und sollte Hochschulen bundesweit Anlass geben, ihre Kontrollsysteme grundlegend zu hinterfragen.

I. Proctoring

Spätestens seit der COVID-19-Pandemie sind Online-Prüfungen aus dem Hochschulalltag nicht mehr wegzudenken. Eine besondere Herausforderung stellt dabei die Überwachung von Täuschungsversuchen dar. Um sicherzustellen, dass Studierende keine unerlaubten Hilfsmittel einsetzen, greifen Universitäten teilweise auf sogenanntes „Proctoring" zurück. Gemeint ist eine Überwachung der Prüflinge über Webcam, Mikrofon und Eingriffe in den Computer der Studierenden. Bei der Überwachung kommen zum Teil menschliche Proctor:innen zum Einsatz, die das Prüfungsgeschehen live beobachten. Andere Hochschulen setzen auf KI-basierte oder hybride Proctoring-Systeme. Konkret geht es um Gesichts- und Verhaltenserkennung, Stimmerkennung, Analyse des Tippverhaltens, Überwachung und Einschränkung von Funktionen der Rechner der Prüflinge.

Unabhängig von der konkreten Ausgestaltung ist klar: Eine solche Überwachung ist datenschutzrechtlich relevant!

Bereits 2021 gab es Verfahren wegen Proctoring beim Oberverwaltungsgericht Schleswig[3] und beim Oberverwaltungsgericht Münster.[4] Beide Verfahren blieben erfolglos. Allerdings handelte es sich um Eilanträge im Normenkontrollverfahren. Mit Urteil vom 17.11.2025 (Az. 3 U 885/24)[5] entschied das Thüringer OLG nun über die datenschutzrechtliche Rechtmäßigkeit eines Proctoring-Systems an der Universität Erfurt.[6] Das Gericht kommt zu dem Ergebnis, dass die Universität mit dem Einsatz eines Proctoring-Systems gegen die Datenschutz-Grundverordnung (DSGVO) verstoßen hat.

II. Der Fall beim Thüringer OLG

Eine Studentin der Universität hatte auf Schadensersatz geklagt, da sie die digitale Überwachung während ihrer Online-Prüfungen als psychisch belastend empfand. Zum Einsatz kam die Software „WISEflow", die mittels automatischer Gesichtserkennung einen kontinuierlichen Abgleich mit einem Referenzbild durchführt.

---

1 Zu Proctoring im Zuge der COVID-19 Pandemie bereits: Uphues, Der Prüfling – Allein zu Haus, DFN-Infobrief Recht 07/2020 und Rennert, Drum prüfe, wer sich online schindet, DFN-Infobrief Recht 10/2022.

2 Abrufbar unter: https://www.juris.de/static/infodienst/autoren/D_NJRE001628443.htm (alle Links dieses Beitrags wurden zuletzt abgerufen am 15.04.2026).

3 OVG Schleswig, Beschluss vom 03.03.2021 – 3 MR 7/21 https://openjur.de/u/2323737.html.

4 OVG Münster, Beschluss vom 4.3.2021 – 14 B 278/21.NE https://openjur.de/u/2323867.html.

5 Abrufbar unter: https://www.juris.de/static/infodienst/autoren/D_NJRE001628443.html.

6 Über das Urteil sprach auch Dr. Jan K. Kocher bei der DFN-Betriebstagung am 18. März 2026 in Berlin. Folien abrufbar unter: https://www.dfn.de/wp-content/uploads/2026/03/BT84_Forum_Recht_Vortrag_Koecher_Rechtsprechung.pdf.

Zusätzlich wurde ein Lock-Down-Browser[7] installiert. Die Klägerin gab an, sich durch die ständige Beobachtung unter Druck gesetzt gefühlt zu haben, da sie befürchtete, bereits alltägliche Bewegungen könnten fälschlicherweise als Betrugsversuch gewertet werden.

Dem Schadensersatzverlangen der Klägerin gab das OLG (anders als die Vorinstanz[8]) statt, wenn auch nur i. H. v. 200 Euro anstatt der geforderten 1.000 Euro.

Durch den automatisierten Abgleich der Live-Bilder mit dem Referenzbild wurden biometrische Daten (Art. 4 Nr. 14 DSGVO)[9] der Klägerin verarbeitet. Diese Verarbeitung war rechtswidrig, da das grundsätzliche Verarbeitungsverbot für biometrische Daten aus Art. 9 Abs. 1 DSGVO betroffen war und keiner der in Art. 9 Abs. 2 DSGVO genannten Ausnahmetatbestände vorlag. Insbesondere hatte die Studentin nicht in die Verarbeitung gem. Art. 9 Abs. 2 lit. a DSGVO ausdrücklich eingewilligt. Die bloße Entscheidung der Klägerin für eine Online-Prüfung sowie die Hinnahme technischer Abläufe, wie etwa die Erstellung eines Referenzbildes, würde keine rechtlich ausreichende Zustimmung zur Verarbeitung biometrischer Daten darstellen. Da eine solche Einwilligung zwingend eine explizite Belehrung über den Einsatz der Gesichtserkennung und eine darauf bezogene, eindeutige Erklärung erfordern würde, genüge weder ein vermeintlich schlüssiges Verhalten der Klägerin noch der allgemeine Verweis auf universitäre Auskunftsstellen den gesetzlichen Anforderungen.

Die Verarbeitung sei auch nicht nach Art. 9 Abs. 2 lit. e DSGVO zulässig. Das Hochladen von Fotos in sozialen Medien stelle keine offensichtliche Veröffentlichung biometrischer Daten dar. Die Klägerin habe damit lediglich Bildmaterial zugänglich gemacht; die eigentliche Gewinnung biometrischer Daten aus diesen Bildern sei ein separater technischer Vorgang, der nicht von ihrer Veröffentlichungshandlung gedeckt sei.

Zwar mag die Durchführung der Prüfung einem gewissen öffentlichen Interesse entsprochen haben, die Verarbeitung der biometrischen Daten sei aber in Anbetracht der Eingriffsintensität und des Bestehens anderer Prüfungsmöglichkeiten jedenfalls nicht erforderlich, sodass auch eine Rechtfertigung über Art. 9 Abs. 2 lit. g DSGVO nicht in Betracht kam.

Für die psychischen Belastungen, die die Klägerin erlitt, sprach das Gericht immateriellen Schadensersatz zu.

Einen weitergehenden Schadensersatz aufgrund von Kontrollverlust lehnte das Gericht allerdings mit der Begründung ab, dass die Klägerin durch das Hochladen von Fotos auf Instagram, die zur Gewinnung biometrischer Daten geeignet sind, selbst bereits die Kontrolle über diese Daten aufgegeben hätte.

III. Rechtliche und technische Hürden beim Proctoring

Spätestens nach diesem Urteil sollte allen Verantwortlichen klar sein, dass die Datenschutzkonformität von Online-Prüfungsformaten genau kontrolliert werden muss. Vielfach dürften Proctoring-Lösungen von Hochschulen gegen die DSGVO verstoßen haben. Dabei ist nicht nur die fehlende Einwilligung zur Verarbeitung biometrischer Daten ein Fallstrick. Auch der Umfang und die Dauer von Speicherungen können etwa in Konflikt mit dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) geraten.[10]

Außerdem ist der Datenschutz nicht die einzige problematische Facette des Proctorings. Teilweise geforderte Raumscans greifen womöglich in die Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG ein.[11] Die von den Studierenden zu installierende Software kann zudem erhebliche IT-Sicherheitsfragen aufwerfen.[12]

---

7 Ein Lockdown-Browser ist ein spezieller Browser, der bei Online-Prüfungen an Hochschulen eingesetzt wird, um Betrug zu verhindern, indem er den Zugriff auf prüfungsfremde Inhalte blockiert, etwa durch das Sperren neuer Tabs oder Fenster.

8 LG Erfurt, Urteil vom 23.10.2024 – 8 O 1117/22.

9 Art. 4 Nr. 14 DSGVO: „…"biometrische Daten" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.".

10 Birnbaum in Birnbaum, Bildungsrecht in der Corona-Krise 1. Auflage 2021, § 4 Hochschule, Rn. 81 ff.

11 https://verfassungsblog.de/grundrechtseingriffe-durch-online-proctoring/, gegenteiliger Auffassung: OVG Schleswig, Beschluss vom 03.03.2021 - 3 MR 7/21 https://openjur.de/u/2323737.html.

12 https://freiheitsrechte.org/uploads/publications/Digital/GFF_IT-Gutachten_Proctoring-Spaehsoftware-gegen-Studierende.pdf.

Ein weiteres Problem, das sich generell beim Einsatz von KI-Systemen stellt, ist mögliche Diskriminierung.[13]

Auch die jeweiligen landesrechtlichen Regelungen des Hochschulrechts[14] sind zu beachten.

Angesichts der rechtlichen Risiken, technischen Herausforderungen und ethischen Bedenken ist es unerlässlich, dass Online-Prüfungen nicht nur täuschungsfrei, sondern auch sensibel in Hinblick auf die Rechte und Interessen von Studierenden ausgestaltet werden.

13 Die von der Uni Erfurt verwendete Software „WISEflow", griff beispielsweise auf „Rekognition" von Amazon Web Services zurück. Dieses Produkt hat in einer Studie des MIT aus 2019 rassistische und sexistische Tendenzen aufgewiesen. https://hochschulforumdigitalisierung.de/pruefungen-in-der-pandemie-online-proctoring-ist-keine-loesung/
Ebenso bestehen Bedenken, dass Proctoring-Software Menschen mit Behinderungen und neurodivergente Menschen diskriminiert. https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/.

14 z. B. §§ 32a, 32b Landeshochschulgesetz (LHG) Baden-Württemberg; §§ 16 ff. Hochschul-Digitalverordnung (HDVO) Nordrhein-Westfalen. Viele landesrechtliche Regeln betrafen allerdings auch lediglich die „Notlösungen" während der COVID-19-Pandemie und sind mittlerweile außer Kraft getreten. Für eine umfassende Darstellung landesrechtlicher Gegebenheiten siehe Rennert, Drum prüfe, wer sich online schindet, DFN-Infobrief Recht 10/2022.

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 Humboldt-Universität Berlin.

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

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

Tel. (030) 838-66754

E-Mail: recht@dfn.de

Podcast der Forschungsstelle Recht im DFN

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: https://anchor.fm/fsr-dfn