„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

9 / 2024
September 2024

Systemische Risiken riesiger Systeme

Sehr große Online-Plattformen müssen unter dem DSA systemische Risiken erkennen und bekämpfen

Künstliche Intelligenz – keine Innovation ohne Diskretion?

DSK-Orientierungshilfe zu Künstlicher Intelligenz und Datenschutz

Just put your hand on your heart and whistle

Deutschland setzt mit der Verabschiedung des Hinweisgeberschutzgesetzes die EU-Whistleblower-Richtlinie 2019/1937 um

Wie geht`s eigentlich Hanna?

Mit der Reform des Wissenschaftszeitvertragsgesetzes sollen die Befristungsregelungen von Wissenschaftler:innen geändert werden

Systemische Risiken riesiger Systeme

Sehr große Online-Plattformen müssen unter dem DSA systemische Risiken erkennen und bekämpfen

von Nikolaus von Bernuth, Berlin

Seit einem Jahr gelten die spezifischen Regelungen des Digital Services Act (DSA) für sehr große Online-Plattformen und Suchmaschinen. Das Herzstück bilden Pflichten zum Umgang mit systemischen Risiken, wie etwa Suchtpotenzial oder der Verbreitung von Hetze und Desinformation. Allerdings besteht ein erhebliches Risiko, dass die Plattformen ihre neuen Pflichten nur unzureichend umsetzen, um ihre lukrativen Geschäftsmodelle zu schützen.

I. Die Macht der sehr großen Online-Plattformen

Es gehört mittlerweile zu den Binsenweisheiten der netzpolitischen Debatte, auf die Macht der sehr großen Online-Plattformen und Suchmaschinen hinzuweisen. Sie sind nicht nur Dienste, mithilfe derer Menschen individuell miteinander kommunizieren und Inhalte teilen. Das Internet und Online-Plattformen im Speziellen sind zu einer der meistgenutzten Quellen für Nachrichten geworden. Im Jahr 2024 verwendet jede:r Dritte in Deutschland zum Empfang von Nachrichten im Internet neben Online-Auftritten klassischer Medien auch soziale Netzwerke.[1] In der Altersgruppe bis 35 Jahre ist es sogar die Hälfte.

Welche Inhalte diese Menschen zu sehen bekommen, richtet sich nicht nur danach, wem sie selbst und ihr eigenes Netzwerk folgen. Maßgeblich werden die Inhalte auf den Online-Plattformen durch Algorithmen und Empfehlungssysteme zusammengestellt. Diese wiederum sind darauf ausgerichtet, das werbegestützte Geschäftsmodell zu optimieren. Der DSA will diese Algorithmen und Empfehlungssysteme transparenter machen.[2] Die zentralen Parameter müssen in den Allgemeinen Geschäftsbedingungen (AGB) bekannt gemacht werden (Art. 27 Abs. 1 DSA). Bei sehr großen Plattformen muss eine Option ohne Profiling wählbar sein (Art. 38 DSA). Dennoch: Für einzelne Nutzende bleibt der Einfluss begrenzt. Dies gilt umso mehr für Plattformen bzw. Funktionen wie TikTok, Instagram Reels oder YouTube Shorts, die ihre Inhalte fast ausschließlich aufgrund von Algorithmen zusammenstellen.

Die sehr großen Online-Plattformen (und Suchmaschinen) haben eine kaum zu überschätzende Bedeutung für die öffentliche Meinungsbildung und Debatte – und durch ihre Algorithmen entsprechende Macht darüber. Mit dem DSA ist es der EU nun erstmals gelungen, spezifische Regelungen einzuführen, die diese Machtverhältnisse und die hiervon ausgehenden gesellschaftlichen Gefahren in den Blick nehmen. Dieser Beitrag wird die Pflichten zur Ermittlung, Analyse, Bewertung und anschließenden Minderung systemischer Risiken auf Online-Plattformen und Suchmaschinen in Art. 34, 35 DSA näher erläutern. Zunächst bietet sich in diesem Zusammenhang aber die Gelegenheit zu erläutern, wen genau die neuen Regelungen betreffen.

II. Was genau sind sehr große Online-Plattformen?

Der DSA verfolgt einen risikobasierten Ansatz. Das intensivste Pflichtenprogramm trifft also nur wenige Adressaten, von denen

1 Reuters Institute Digital News Report 2024: Ergebnisse für Deutschland, S. 16f, https://www.ssoar.info/ssoar/handle/document/94461 (zuletzt abgerufen am 14.08.2024).

2 Grundlegend zum DSA: Gielen, Digital Services Act: Das Plattformgrundgesetz?, DFN-Infobrief Recht 03/2021; Rennert, Brüssel reguliert das schon, DFN-Infobrief Recht 06/2022; John, Geschenke verpacken leicht gemacht: Transparenz ist in!, DFN-Infobrief Recht 12/2023; siehe auch von Bernuth, Kurzbeitrag: The floor is yours, Bundesnetzagentur, DFN-Infobrief Recht 08/2024.

nach Ansicht des Gesetzgebers eine besonders hohe Gefahr ausgeht. Dies sind Online-Plattformen und Online-Suchmaschinen mit mehr als 45 Mio. aktiven monatlichen Nutzende in der EU (Art. 33 Abs. 1 DSA).[3]

Online-Plattformen sind solche Vermittlungsdienste, die Informationen im Auftrag ihrer Nutzenden speichern und öffentlich verbreiten und bei denen dies keine unwesentliche Nebenfunktion darstellt (Art. 3 lit. i DSA).[4] Dazu gehören etwa soziale Netzwerke, Videosharing-Plattformen oder Online-Marktplätze. Aber auch Wikipedia als Online-Enzyklopädie oder Google Maps als Kartendienstleister fallen in die Kategorie Online-Plattform. Messengerdienste wie WhatsApp oder Signal hingegen verbreiten die Informationen (bspw. eine Chatnachricht) nicht öffentlich, jedenfalls nicht an eine beliebige Öffentlichkeit. Sie sind also nur Dienste der reinen Durchleitung von Informationen und keine Online-Plattformen. Ein Spezialfall ist Telegram: Anfangs stand die Individualkommunikation hier ebenfalls im Fokus. Doch seit einiger Zeit werden die Kanäle, auf denen Inhalte an eine beliebige Öffentlichkeit verbreitet werden können, immer bedeutsamer und prägender für den Dienst. Sie sind (nicht nur, aber auch) zentrale Sprachrohre für rechte Hetze, Verschwörungstheorien oder Desinformationskampagnen.[5] Daher ist die öffentliche Verbreitung keine unwesentliche Nebenfunktion mehr – Telegram ist eine Online-Plattform. Streitig ist bislang aber, ob Telegram genug Nutzende hat, um sich auch an die strengsten Pflichten des DSA halten zu müssen, unter anderem also die Pflichten zur Risikobewertung und Risikominderung.[6]

Suchmaschinen sind keine Online-Plattformen, denn ihr Service besteht nicht in der öffentlichen Verbreitung von Informationen, sondern der Such- und Auflistungsfunktion.[7] Für Suchmaschinen mit über 45 Mio. aktiven Nutzende (zurzeit: Google Search und Bing) gelten die besonders strengen Pflichten der Art. 33-48 DSA aber ebenfalls.

III. Haftungsbefreiung für Freiheit im Netz

Über viele Jahre konnten sich die großen Online-Plattformen in einem ausgesprochen innovationsfreundlichen Rechtsrahmen entwickeln und waren kaum Haftungsrisiken und Sorgfaltspflichten ausgesetzt. Die E-Commerce-Richtlinie von 2001 sah eine weitgehende Haftungsbefreiung vor: Online-Plattformen waren für Inhalte, die Nutzende hochgeladen hatten, regelmäßig nicht verantwortlich.

Der DSA hält an diesem Grundkonzept fest. Eine grundsätzliche Haftungsprivilegierung ist erforderlich, damit die Kommunikationsfreiheiten so ausgeübt werden können, wie es mittlerweile selbstverständlich ist. Würden Online-Plattformen unmittelbar für alle Inhalte haften, wäre ein freier, ungefilterter Austausch von Inhalten undenkbar.
Dennoch hat sich gezeigt, dass die Plattformen mehr Verantwortung tragen müssen. Die Gefahren, die die Freiheit im Netz zwangsläufig mit sich bringt, zeigten sich in den vergangenen Jahren immer deutlicher. Hassrede, systematische Rechtsverletzungen und Desinformation haben spürbar zugenommen – ihre Auswirkungen zeigen sich etwa in sensiblen demokratischen Momenten wie Wahlen oder gesellschaftlichen Krisen.[8] Verschärft werden diese Gefahren durch die spezifische Funktions- und Wirkweise der sehr großen Online-Plattformen. An genau dieser Stelle setzen die Pflichten zur Risikobewertung und Risikominderung in Art. 34, 35 DSA an.

---

3 Zur Anwendbarkeit ist eine Benennung durch die Europäische Kommission erforderlich. Die Liste aller 25 bisher benannten Online-Plattformen und Suchmaschinen findet sich hier: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (zuletzt abgerufen am 15.08.2024).

4 Eine unwesentliche Nebenfunktion sind etwa die Kommentarspalten in Online-Auftritten einer Zeitung, so explizit Erwägungsgrund 13 DSA.

5 Telegram ist etwa zentrales Medium der rechtsextremen „Freien Sachsen“, ebenfalls für russische Propaganda: https://correctiv.org/faktencheck/hintergrund/2024/04/10/telegram-analyse-desinformation-russland-vernetzt-sich-um-alina-lipp-in-deutschland-mit-propaganda-fakes-zum-ukraine-krieg/ (zuletzt abgerufen am 15.08.2024).

6 Telegram meldete „nur“ 41 Mio. aktive Nutzer:innen, die EU-Kommission zweifelt aber an diesen Zahlen, https://www.inside-it.ch/eu-nimmt-sich-wohl-telegram-an-20240529# (zuletzt abgerufen am 15.08.2024).

7 Im Einzelnen ist die Kategorisierung von Suchmaschinen sehr streitig. Definiert werden Online-Suchmaschinen in Art. 3 lit. j DSA. Der Übersichtlichkeit halber wird im weiteren Beitrag hinsichtlich der Adressaten der Art. 34, 35 DSA von (Online-)Plattformen gesprochen, wobei Suchmaschinen mit eingeschlossen sind.

8 Dem Brexit-Referendum sowie der Wahl Donald Trumps 2016 wird nachgesagt, durch Desinformation erheblich beeinflusst worden zu sein. Exemplarisch sind auch die jüngsten Ausschreitungen in Großbritannien.

IV. Systemische Risiken

Nach Art. 34 Abs. 1 DSA müssen die benannten sehr großen Online-Plattformen ermitteln, welche systemischen Risiken von dem Betrieb ihrer Dienste ausgehen, und diese anschließend analysieren und bewerten. Mindestens einmal jährlich muss die Risikobewertung erfolgen, sowie stets dann, wenn die Plattform eine neue Funktion mit Risikopotenzial einführt.[9]

Der Begriff systemische Risiken ist aus der Bankenregulierung bekannt.[10] Systemische Risiken sind mehr als nur die Summe der einzelnen Beschwerden und Rechtsverstöße, die an die Plattformen herangetragen werden. Das Ziel ist insbesondere die Ermittlung struktureller Risiken, die mit dem Betrieb sehr großer digitaler Dienste einhergehen und die sich aus der Analyse des eigenen Dienstes und den – ohnehin gesammelten – Nutzungsdaten ergeben: Welche Gefahren oder negative Auswirkungen treten immer wieder auf und lassen sich auf die Funktionsweise des eigenen Dienstes zurückführen? „Systemisch" stellt zudem einen Bezug zur europäischen Grundordnung her, die in ihrer Funktionsfähigkeit oder Stabilität durch diese Risiken gefährdet sein muss. Der DSA gibt vier Kategorien von systemischen Risiken auf Online-Plattformen vor (Art. 34 Abs. 1 DSA).

Erstens ist dies die Verbreitung rechtswidriger Inhalte über den Dienst. Rechtswidrig sind alle Inhalte, die gegen das Unionsrecht oder das Recht eines Mitgliedstaats verstoßen. Typischerweise wird es etwa um die Verbreitung von strafbarer Hassrede, Missbrauchsdarstellungen auf Videosharing-Plattformen oder den massenhaften Verkauf gefälschter Güter gehen.[11] Plattformen müssen also prüfen, ob ihre Funktionsweise gerade solche Praktiken besonders begünstigt bzw. systematisch zulässt.

Zweitens sind dies die tatsächlichen oder absehbaren Auswirkungen auf die Ausübung der Grundrechte. Hier soll ausweislich der Erwägungsgründe der Fokus insbesondere auf der Meinungsfreiheit, dem Recht auf Nichtdiskriminierung sowie Jugendschutz liegen. Aber auch die Auswirkungen auf andere Grundrechte durch die Funktionen und Algorithmen der Plattformen sollen beobachtet werden.

Drittens werden als systemische Risiken die Auswirkungen auf die gesellschaftliche Debatte, auf Wahlprozesse und die öffentliche Sicherheit definiert. Hierunter wird in der rechtswissenschaftlichen Literatur insbesondere Desinformation eingeordnet, außerdem Phänomene wie Filterblasen und Echokammern.[12] An dieser Stelle findet sich also eine der wenigen gesetzlichen Regelungen zu Desinformation, die in den Erwägungsgründen des DSA als eine der zentralen Gefahren auf Online-Plattformen ausgemacht wird. [13]

Zuletzt fallen unter die vierte Kategorie systemischer Risiken die nachteiligen Auswirkungen auf geschlechtsspezifische Gewalt, öffentliche Gesundheit, Jugendschutz oder das körperliche und geistliche Wohlbefinden einer Person. In diese Kategorie fällt etwa das Suchtpotenzial (gerade für Jugendliche), das von der Gestaltung vieler Online-Plattformen ausgeht. Außerdem kann auch hier laut den Erwägungsgründen Desinformation ein Risikofaktor sein – etwa für die öffentliche Gesundheit, wie es sich während der Coronapandemie eindrücklich gezeigt hat.

Die Auflistung systemischer Risiken ist nicht abschließend. Weil die benannten Risiken aber sehr weit formuliert sind (etwa „Auswirkungen auf die Grundrechte"), werden sie einen erheblichen Teil der systemischen Risiken der sehr großen Online-Plattformen erfassen.

V. Ermitteln, Analysieren und Bewerten

Zur Ermittlung systemischer Risiken gibt der DSA außerdem besonders relevante Parameter zur Hand, die die Plattformen analysieren müssen. Dies sind (Art. 34 Abs. 2 DSA):

---

9 Gegen die Prüfpflicht bei Einführung verstieß aus Sicht der Kommission TikTok Lite, zum Hintergrund siehe https://ec.europa.eu/commission/presscorner/detail/de/IP_24_2227 (zuletzt abgerufen am 15.08.2024).

10 Einen Vergleich zu diesem Sektor ziehend: Broughton Micova/Calef, Elements for Effective Risk Assessment under the DSA, 2023, https://www.ssrn.com/abstract=4512640 (zuletzt abgerufen am 15.08.2024).

11 Aufschlussreich für die Auslegung der systemischen Risiken sind die Erwägungsgründe 80-84 zum DSA.

12 *Kaesling*, in: Hofmann/Raue, Digital Services Act, 1. Auflage, 2023, Art. 34 DSA, Rn. 102ff; siehe auch das erste förmliche Verfahren gegen X: https://ec.europa.eu/commission/presscorner/detail/de/ip_23_6709 (zuletzt abgerufen am 15.08.2024).

13 Erwähnung findet Desinformation in den Erwägungsgründen 2, 9, 68, 83, 84, 95, 104, 106, 108.

a) die Gestaltung ihrer Empfehlungssysteme und anderer relevanter algorithmischer Systeme,
b) ihre Systeme zur Moderation von Inhalten,
c) ihre anwendbaren allgemeinen Geschäftsbedingungen und ihre Durchsetzung,
d) Systeme zur Auswahl und Anzeige von Werbung,
e) ihre datenbezogene Praxis.

In ihren jährlichen Berichten müssen die Plattformen jedenfalls hinsichtlich dieser explizit benannten Parameter für die Risikobewertung Rechenschaft ablegen. Sie müssen also beispielsweise darlegen, inwieweit ihre Empfehlungssysteme zur Verbreitung von Desinformation beitragen oder zu Sucht- und Abhängigkeitsverhalten führen. Dies wurde TikTok Lite zum Verhängnis: Aus Sicht der Kommission hat TikTok die Suchtrisiken der Funktion, die mit Belohnungssystemen arbeitet, nicht ausreichend untersucht – inzwischen hat TikTok die Funktion auf dem europäischen Markt gänzlich zurückgezogen.[14] Auch gegen Facebook und Instagram läuft ein Verfahren, weil diese das Suchtpotenzial der Dienste nicht ausreichend analysiert haben.[15]

Im Übrigen gibt es mangels Erfahrungen mit den neuen Sorgfaltspflichten noch wenig Beispielsfälle, aus denen sich ableiten lässt, wie eine Risikoermittlung, Analyse und Bewertung durch die Plattformen im Detail auszusehen hat. In der Zivilgesellschaft finden sich schon einige Vorschläge,[16] entscheidend wird aber der von den Plattformen beschrittene Weg sein. Die Pflichten folgen dem Prinzip überwachter Selbstregulierung. Die Plattformen ermitteln und bewerten ihre systemischen Risiken eigenständig. Insbesondere ist es ihnen überlassen, welche Konsequenzen sie aus den ermittelten systemischen Risiken ableiten. Diese Selbstregulierung ist aber überwacht: Sie müssen sich unabhängigen Prüfungen unterziehen (Art. 37 DSA) und unterliegen der Aufsicht durch die Kommission.

VI. Eigenständige Risikominderung

Art. 35 DSA verpflichtet die Online-Plattformen dazu, wirksame und angemessene Maßnahmen zu ergreifen, um die ermittelten systemischen Risiken zu reduzieren. Welche dies sind, kann die Plattform selbst entscheiden – dies ist auch Ausdruck ihrer unternehmerischen Freiheit. Die Maßnahmen müssen aber auf die ermittelten Risiken zugeschnitten sein. Art. 35 Abs. 1 DSA schlägt eine ausführliche Liste von möglichen Maßnahmen vor. Er umfasst unter anderem die Anpassung von Online-Schnittstellen, Empfehlungssystemen und Algorithmen, der Werbesysteme sowie eine Kennzeichnung für manipulierte Inhalte.

Wenn die Plattform also beispielsweise feststellt, dass die automatisierte Inhaltemoderation durch Nutzung algorithmischer Filtersysteme[17] zu einem fortdauernden Overblocking eigentlich rechtmäßiger Inhalte führt, muss sie hierin ein systemisches Risiko für die Meinungsfreiheit der Nutzenden erkennen. Sie muss dann etwa das algorithmische System verbessern oder verstärkt Entscheidungen durch Mitarbeitende überprüfen lassen. Sollte hingegen ein Underblocking (rechtswidrige Inhalte werden nicht erkannt) Ergebnis der Risikoanalyse sein, müsste auch darauf gerichtet der Algorithmus verbessert werden.

Bei allen Minderungsmaßnahmen haben die Plattformen die Auswirkungen auf die Grundrechte besonders zu berücksichtigen. Daher gilt es, unnötige Beschränkungen für die Nutzung der Dienste zu vermeiden.[18] Die Minderungsmaßnahmen müssen zum Ziel haben, nicht einzelne Nutzende von der Plattform auszuschließen oder den Dienst insgesamt auszusetzen, sondern die Plattform so zu gestalten, dass es möglichst wenig Anlass für Sperrmaßnahmen gibt.

Aufschlussreich ist auch, dass der Gesetzgeber den Terminus Risikominderung und nicht etwa Beseitigung gewählt hat. Eine vollständige Beseitigung eines Risikos geht regelmäßig mit ungewollten grundrechtlichen Einschnitten einher. So könnte eine vollständige Filterung von Nachrichtenbeiträgen nicht

14 https://ec.europa.eu/commission/presscorner/detail/en/IP_24_4161 (zuletzt abgerufen am 15.08.2024).

15 https://ec.europa.eu/commission/presscorner/detail/de/ip_24_2664 (zuletzt abgerufen am 15.08.2024).

16 AlgorithmWatch: https://algorithmwatch.org/en/wp-content/uploads/2023/08/AlgorithmWatch_Risk_Assessment-DSA.pdf; cerre: https://cerre.eu/wp-content/uploads/2023/07/CERRE-DSA-Systemic-Risk-Report.pdf (zuletzt abgerufen am 15.08.2024).

17 Zur Zulässigkeit nach Urteil des EuGH vom 26.04.2022 (Az. C 401/19) siehe Schaller, Alea iacta est: Uploadfilter bleiben, DFN-Infobrief Recht 08/2022.

18 Erwägungsgrund 86 S. 3 DSA.

verifizierter Accounts vor Desinformation schützen – der Eingriff in die Presse- und Meinungsfreiheit wäre aber enorm. Für eine gute Balance soll eine Maßnahme die identifizierten Risiken also nicht zwangsläufig beseitigen, sondern in grundrechtssensibler Weise mindern.

VII. Aufsicht

Wirksam ist der Pflichtenkatalog nur dann, wenn die Aufsicht effektiv und kompetent ist. Das Risikomanagement des DSA schlägt viel vor, verpflichtet aber zu wenig Konkretem. Die Plattformen können nicht nur über die Maßnahmen eigenständig befinden, sie sind auch diejenigen, die die Bewertungsgrundlage dafür schaffen, indem sie ihre systemischen Risiken eigenständig analysieren. Das macht die Beaufsichtigung höchst komplex. Es wird wohl einige Jahre brauchen, bis die Aufsichtsbehörden aus einer vergleichenden Analyse der Praxis verschiedener Plattformen ableiten können, welche Plattform ihr Risikomanagement ernst nimmt und welche nicht.

Zuständig für die Aufsicht über die Pflichten gem. Art. 34, 35 DSA ist die Europäische Kommission. Sie kann Bußgelder von bis zu sechs Prozent des Jahresumsatzes verhängen, je nach Plattform also zweistellige Milliardenbeträge. In den ersten Monaten zeigte sie sich als äußerst engagierte Aufsichtsbehörde, die bereits eine Vielzahl an Verfahren gegen die sehr großen Plattformen einleitete. Manche von ihnen hatten auch die Pflichten zum Risikomanagement zum Gegenstand, unter anderem in den genannten Verfahren gegen TikTok, Meta und X.[19] Das Gremium für digitale Dienste[20] wird mit der Kommission in Kürze auch den ersten Bericht veröffentlichen, der die wesentlichen Erkenntnisse nach einem Jahr Aufsicht über das Risikomanagement der Plattformen enthält.

VIII. Bedeutung für die Wissenschaft und Fazit

Online-Plattformen sind für die moderne Informationsgesellschaft zentral. Insofern profitiert auch die Wissenschaft von sicheren Online-Plattformen, auf denen sich Menschen frei austauschen können und die nicht von Desinformation, Verschwörungstheorien und Hetze geprägt sind. Viele Studierende beziehen auch Studieninhalte über sehr große Online-Plattformen. Spezifische Rechte oder Pflichten in Bezug auf die Wissenschaft enthalten Art. 34, 35 DSA nicht. Allerdings könnte die Forschung von den Informationen profitieren, die aus den Berichten über das Risikomanagement hervorgehen werden. Sie dürften wertvolle Einblicke in den Maschinenraum der Plattformen geben.

Daneben bleibt der Datenzugang für Forschende nach Art. 40 DSA die wichtigste DSA-Regelung für die Wissenschaft.[21] Er ermöglicht es, die systemischen Risiken der Plattformen genauer zu erforschen. Zu diesem Zweck können Forschende bei der Bundesnetzagentur eine Zulassung für einen solchen Datenzugang beantragen, bei Erfüllung aller Kriterien (Art. 40 Abs. 8 DSA) vermittelt sie dann den Zugang.[22]

Der DSA hat für die sehr großen Online-Plattformen und Suchmaschinen anspruchsvolle Pflichten etabliert, deren Herzstück die Pflichten zur Risikobewertung und Risikominderung sind. Nehmen die Plattformen ihre Verantwortung ernst, ist das Potenzial beachtlich. Es scheint möglich, durch die gezielte Verbesserung von Funktionen, Algorithmen und Empfehlungssystemen, die Risiken, die von den Plattformen ausgehen, maßgeblich zu reduzieren. Fraglich ist allein, ob die Plattformen eigenständig ausreichende Maßnahmen ergreifen werden. Sie haben nicht zufällig die heutige Form angenommen, sondern wurden konsequent zur Optimierung ihres werbegestützten Geschäftsmodells gestaltet. Systemische Risiken wie Suchtverhalten sind aus plattformökonomischer Perspektive Chancen, den eigenen Gewinn zu steigern. Daher wird der Erfolg der neuen Pflichten ganz entscheidend von der Qualität der Aufsicht abhängen. Das Handeln der Kommission weckt hier nach der ersten Jahresbilanz durchaus Hoffnung.

---

19 Auch AliExpress und diverse Plattformen mit pornografischen Inhalten sind von Verfahren betroffen, https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (zuletzt abgerufen am 15.08.2024).

20 Das Gremium für digitale Dienste setzt sich aus Vertreter:innen der Koordinatoren für digitale Dienste der einzelnen Mitgliedsstaaten sowie der Kommission zusammen, vgl. von Bernuth, Kurzbeitrag: The floor is yours, Bundesnetzagentur, DFN-Infobrief Recht 08/2024.

21 Genauer nachzulesen bei John, Geschenke verpacken leicht gemacht: Transparenz ist in!, DFN-Infobrief Recht 12/2023.

22 Siehe von Bernuth, Kurzbeitrag: The floor is yours, Bundesnetzagentur, DFN-Infobrief Recht 08/2024.

Künstliche Intelligenz – keine Innovation ohne Diskretion?

DSK-Orientierungshilfe zu Künstlicher Intelligenz und Datenschutz

Von Johannes Müller, Münster

Sofern Organisationen über den Einsatz von KI-Anwendungen entscheiden, müssen sie auch die Anforderungen des Datenschutzrechts beachten. Unterschiedliche Rechtsfragen sind noch nicht abschließend geklärt. Unterstützung bei der Auswahl von KI-Anwendungen kann die Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)[1] geben, die unterschiedliche datenschutzrechtliche Herausforderungen beleuchtet.

I. Datenschutzrechtlicher Klärungsbedarf beim Einsatz von KI

Bei der Auswahl einer KI-Anwendung müssen Organisationen auch beachten, ob der konkrete Einsatz einer Anwendung gegen das geltende Recht verstößt. Rechtliche Fragestellungen können sich aus unterschiedlichen Rechtsgebieten ergeben, etwa dem Urheberrecht oder Arbeitsrecht. Zukünftig wird auch die KI-Verordnung zu beachten sein.[2] Sofern bei der Nutzung der Anwendung oder gegebenenfalls auch beim Training des KI-Modells personenbezogene Daten verarbeitet werden, ist zudem das Datenschutzrecht einschlägig. Aus datenschutzrechtlicher Perspektive kommen eine Vielzahl konkreter Einzelfragen in Betracht, die weiterer Klärung bedürfen. Daher sind Stellungnahmen der Datenschutzbehörden unverzichtbar, die weitere Rechtsklarheit verschaffen können. Einzelne Behörden haben sich bereits zu unterschiedlichen konkreten Fragen geäußert. Jüngst hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg einen Orientierungshilfen-Navigator KI & Datenschutz veröffentlicht, der übersichtlich tabellarisch darstellt, zu welchen konkreten datenschutzrechtlichen Fragen sich die bestehenden Stellungnahmen äußern.[3]

Im Folgenden soll die Orientierungshilfe der DSK „Künstliche Intelligenz und Datenschutz“ Version 1.0, vom 6. Mai 2024 vorgestellt werden. Sie zeichnet sich besonders dadurch aus, dass sie nicht lediglich die Rechtsauffassung eines spezifischen Landesbeauftragten für Datenschutz wiedergibt. Stattdessen stellen die Orientierungshilfen der DSK eine gemeinsame Position dar, auf die sich Datenschutzaufsichtsbehörden des Bundes und der Länder verständigt haben.[4]

---

1 Die Orientierungshilfe kann abgerufen werden unter https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf (zuletzt abgerufen am 05.08.2024).

2 Vgl. Schöbel, Europäische Sandkästen für KI, DFN-Infobrief Recht, 08/2024; und zum Entwurf Rennert, One KIss is all it takes, DFN-Infobrief Recht 01/2023.

3 Der Orientierungshilfen-Navigator KI & Datenschutz, kann abgerufen werden unter https://www.baden-wuerttemberg.datenschutz.de/onkida/ (zuletzt abgerufen am 05.08.2024).

4 Vgl. die Geschäftsordnung der DSK, A. III. Aufgaben der Datenschutzkonferenz, abrufbar unter https://www.datenschutzkonferenz-online.de/media/dsk/Geschaeftsordnung_DSK_Stand_Februar-2024.pdf (zuletzt abgerufen am 05.08.2024).

II. Orientierungshilfe für den Einsatz von KI-Anwendungen

Datenschutzrechtliche Herausforderungen können sich sowohl beim Training eines KI-Modells als auch beim Einsatz der KI-Anwendung stellen. Die Orientierungshilfe der DSK beschäftigt sich primär mit letzterem. Sie möchte Kriterien aufzeigen, die zu berücksichtigen sind, wenn KI-Anwendungen eingesetzt werden. Damit soll sie als Leitfaden für die Auswahl, Implementation und Nutzung von KI-Anwendungen dienen. An die Entwickler von KI-Anwendungen richtet sie sich nur mittelbar, Entwicklung und Training des Modells bilden nicht den Schwerpunkt.

Auch wenn die Orientierungshilfe durch ihren Titel zunächst einen weiten Anwendungsbereich in Form unterschiedlichster KI-Anwendungen nahelegt, stellt sie zu Beginn klar, dass sie sich schwerpunktmäßig mit Large Language Models (LLMs) auseinandersetzt.[5] Die Ausführungen sollen aber gegebenenfalls auch auf andere Anwendungen übertragbar sein.

Im Folgenden sollen lediglich ausgewählte Kriterien aus der Orientierungshilfe dargestellt werden, die sich insgesamt aus 24 Unterabschnitten zusammensetzt.

III. Grundentscheidungen bei der Auswahl von KI-Anwendungen

Der Zweckbindungsgrundsatz des Datenschutzrechts erfordert eine Festlegung und Beschränkung der Datenverarbeitung auf einen spezifischen Zweck. Dementsprechend soll eine Organisation auch vor Einrichtung einer KI-Anwendung festlegen, für welche Einsatzfelder sie die Anwendung nutzen möchte. Dies umfasst auch, dass durch interne Weisungen eindeutig bestimmt wird, unter welchen Voraussetzungen und zu welchen Zwecken Beschäftigte eine KI-Anwendung einsetzen dürfen. Ein solcher klarer Rahmen sollte zudem dokumentiert werden.

Öffentliche Stellen, zu denen auch öffentlich-rechtliche Hochschulen zählen, haben zudem zu beachten, dass die Anwendung im Rahmen der gesetzlich zugewiesenen öffentlichen Aufgaben erfolgt.

Eine genaue Festlegung des Einsatzfeldes soll es auch ermöglichen, im Vorhinein zu prüfen, ob das Datenschutzrecht überhaupt einschlägig ist. Sofern, weder die Eingabe-, noch die Ausgabedaten personenbezogene Informationen enthalten und auch nicht der Anmelde- und Verarbeitungsprozess unter Verarbeitung personenbezogener Informationen erfolgt, ist das Datenschutzrecht nicht anwendbar und muss beim Betrieb der Anwendung nicht beachtet werden. Die Orientierungshilfe weist aber darauf hin, dass sich ein Personenbezug aus vielfältigen, unterschiedlichen Merkmalen herleiten lässt und daher einer genauen Überprüfung bedarf.

Die Festlegung eines bestimmten Verarbeitungszwecks, soll auch die Feststellung erleichtern, ob die Verarbeitung gerechtfertigt ist. Sofern mit Hilfe der KI-Anwendung personenbezogene Daten verarbeitet werden sollen, erfordert jede Datenverarbeitung das Vorliegen einer Rechtsgrundlage. Hierbei muss auch berücksichtigt werden, welche Kategorien von Daten verarbeitet werden. Bestimmte Datenkategorien hält die DSGVO für besonders schützenswert und stellt an ihre Verarbeitung gemäß Art. 9 DSGVO strengere Anforderungen. Zudem muss auch bei der Rechtsgrundlage zwischen Datenverarbeitungen von öffentlichen und nichtöffentlichen Stellen differenziert werden. Darüber hinaus verweist die Stellungnahmen bezüglich der unterschiedlichen Rechtsgrundlagen, die in Betracht kommen, auf das Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“[6] des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

Eine weitere Grundentscheidung, die bereits bei der Auswahl der Anwendung getroffen werden muss, betrifft die Frage, ob die KI-Anwendung auf einem geschlossenen oder einem offenen Modell basieren soll. Bei geschlossenen Systemen hat der Anwender die Kontrolle über die Ein- und Ausgabedaten, da die Datenverarbeitung in einer eingegrenzten und technisch abgeschlossenen Umgebung stattfindet. Damit können die Anwender auch gleichzeitig ausschließen, dass die eingegebenen Daten vom Anbieter des Systems zum weiteren Training verwendet werden. Bei offenen Systemen erfolgt die Datenverarbeitung hingegen nicht in einem technisch abgeschlossenen System, etwa auf den Servern des Anwenders. Stattdessen wird die Anwendung auf den Servern des Anbieters betrieben und ist für Anwender über das Internet zugänglich. In einem solchen Fall

5 Vgl. zu Large Language Models, Müller, Zu gut, um menschlich zu sein, DFN-Infobrief Recht 05/2024.

6 Abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/ (zuletzt abgerufen am 05.08.2024).

haben die Anwender naturgemäß eine geringere Kontrolle über die weitere Verwendung der Daten, die sie in die Anwendung eingeben. Es besteht das technische Risiko, dass die eingegebenen personenbezogenen Daten für das Training der KI und die Beantwortung von Anfragen anderer Anwender verwendet werden. Damit können die Anwender nicht technisch ausschließen, dass die eingegebenen personenbezogenen Daten nicht gegenüber unbefugten Dritten offengelegt werden. Gleichzeitig ist damit auch die Eingabe von dienstlichen Informationen, die nicht für die Öffentlichkeit bestimmt sind, in ein offenes System mit besonderen Risiken verbunden. Aufgrund der beschränkten Kontrolle über die weitere Verwendung besteht zudem die Möglichkeit, dass die personenbezogenen Daten in Drittstaaten übertragen werden. Hierfür gelten besonders strenge datenschutzrechtliche Anforderungen. Es verwundert daher nicht, dass die Orientierungshilfe der DSK geschlossene Systeme aus datenschutzrechtlicher Sicht als vorzugswürdig einstuft.

IV. Datenschutzrechtliche Verantwortlichkeit

Die Einhaltung der datenschutzrechtlichen Pflichten trifft grundsätzlichen den Verantwortlichen. Dies ist die Person, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Auch bei der Bestimmung des Verantwortlichen differenziert die Orientierungshilfe zwischen der Nutzung von geschlossenen und offenen KI-Anwendungen.

Sofern eine geschlossene Anwendung ausschließlich zu eigenen Zwecken auf eigenen Servern betrieben wird, ist diese Stelle auch in der Regel der alleinige Verantwortliche der Datenverarbeitung.

Aber auch wenn eine Organisation eine (offene) KI-Anwendung nutzt, die von einem externen Anbieter auf externen Servern betrieben wird, ist die nutzende Organisation in der Regel Verantwortlicher der Datenverarbeitung. Der externe Anbieter handelt dann als verlängerter Arm im Auftrag des Verantwortlichen, sodass in der Regel ein Auftragsverarbeitungsverhältnis gemäß Art. 28, 29 DSGVO vorliegt. Der Verantwortliche hat dann mit dem Anbieter der Anwendung eine Vereinbarung gemäß Art. 28 Abs. 3 DSGVO zu schließen.

Die Orientierungshilfe geht zudem darauf ein, dass die Verantwortlichkeit auch in Form einer gemeinsamen Verantwortlichkeit (Art. 26 DSGVO) vorliegen kann, sofern zwei Stellen eine gemeinschaftliche Entscheidung über die Zwecke und Mittel der Verarbeitung treffen. In einem solchen Fall müssen sie gemäß Art. 26 Abs. 1 S. 2 DSGVO in einer Vereinbarung in transparenter Form festlegen, wer welche Pflichten aus der DSGVO erfüllt.

V. Transparenz

Den Verantwortlichen einer Datenverarbeitung treffen verschiedene Transparenzpflichten. Der Verantwortliche hat etwa gemäß Art. 13 Abs. 1 lit. c, Abs. 2 lit. a DSGVO die betroffene Person zum Zeitpunkt der Datenerhebung über den Zweck und die Dauer der Datenverarbeitung zu informieren. Wenn der Verantwortliche die KI-Anwendung, in dessen Rahmen personenbezogene Daten verarbeitet werden, nicht selbst entwickelt hat, verfügt er häufig nicht über alle Informationen, die zur Erfüllung seiner Transparenzpflichten erforderlich sind. Deshalb weist die Stellungnahme darauf hin, dass der Verantwortliche darauf achten muss, vom Anbieter alle notwendigen Informationen zu erhalten. Die Anbieter müssen hierfür entsprechende Dokumentationen bereitstellen. Regelmäßig wird zwischen dem Anwender und dem Anbieter der Anwendung ein Auftragsverarbeitungsverhältnis vorliegen. Dann ist der Anbieter bereits nach Art. 28 Abs. 3 S. 2 lit. e DSGVO verpflichtet, den Verantwortlichen bei der Erfüllung seiner Transparenzpflichten zu unterstützen.

Sofern die eingegebenen personenbezogenen Daten für das Training der KI weiterverwendet werden, muss auch hierüber die betroffene Person informiert werden.

Aus Transparenzgründen ist es zudem erforderlich, dass Nutzern der Anwendung darüber informiert werden, dass ihre Eingaben zu einem späteren Zeitpunkt von anderen Nutzer eingesehen werden können, sofern diese Möglichkeit besteht. Dies ist vor allem relevant bei der Nutzung einer Anwendung bzw. eines Accounts durch verschiedene Beschäftigte.

VI. Betroffenenrechte

Die Orientierungshilfe weist auch darauf hin, dass Verantwortliche gewährleisten müssen, dass betroffene Personen ihr Recht auf Berichtigung gemäß Art. 16 DSGVO und Löschung gemäß Art. 17 DSGVO ausüben können. Hierfür sollen geeignete technische Verfahren konzipiert werden. Insbesondere bei der Verwendung

personenbezogener Daten für das Training der KI wird die praktische Umsetzung eine Herausforderung darstellen. Als mögliche technische Maßnahmen zur Umsetzung des Rechts auf Berichtigung nennt die Stellungnahme das Nachtraining oder das Fine Tuning der Daten. Bezüglich des Rechts auf Löschung verweist die Stellungnahme auf das Nachschalten von Filtern, die unerwünschte Ausgaben verhindern sollen. Hierdurch werde zwar keine vollkommene Löschung im Sinne von Art. 17 DSGVO umgesetzt, da die Daten weiterhin für das Modell verfügbar sein können. Dennoch käme die Filtertechnologie den Rechten und Freiheiten der betroffenen Person zugute, da hierdurch unerwünschte Ausgaben vermieden werden können.

VII. Relevanz für wissenschaftliche Einrichtungen

Wissenschaftlichen Einrichtungen stellt sich in gleicher Weise wie anderen Organisationen die Frage, wie eine datenschutzkonforme Nutzung von KI-Anwendungen erfolgen kann. Hierbei gibt die Stellungnahme der DSK einen aufschlussreichen Überblick, über unterschiedliche datenschutzrechtliche Herausforderungen und mögliche Lösungen. Vorliegend sollten nur einzelne Punkte dargestellt werden. Weitere Aussagen trifft die Stellungnahme etwa auch zur Konzeption der KI-Systeme, sodass die Anforderungen an eine datenschutzfreundliche Technikgestaltung und die Pflichten zur Datensicherheit eingehalten werden. Aber auch zur konkreten Nutzung der KI-Anwendung erfolgen weitere Ausführungen, etwa auch zur Verhinderung von Diskriminierungen durch die KI-Anwendung.

Neben der DSK-Stellungnahme können sich auch die verschiedenen Orientierungshilfen der Landesdatenschutzbehörden als nützlich erweisen, sofern es eine konkrete datenschutzrechtliche Frage zu beantworten gilt.

Just put your hand on your heart and whistle

Deutschland setzt mit der Verabschiedung des Hinweisgeberschutzgesetzes die EU-Whistleblower-Richtlinie 2019/1937 um

Von Marc-Philipp Geiselmann, Münster

Mit eineinhalb Jahren Verspätung setzt die Bundesrepublik Deutschland die EU-Whistleblower-Richtlinie (RL) mit dem Hinweisgeberschutzgesetz (HinSchG) um. Dieser Beitrag erläutert den Inhalt des Hinweisgeberschutzgesetzes und beantwortet auch die Frage, ob für Hochschulen ein Handlungsbedarf besteht.

I. Gesetzgebungsverfahren

Der Erlass des HinSchG fußt auf der EU-Whistleblower-RL[1] der Europäischen Union, die bis zum 17. Dezember 2021 hätte umgesetzt werden müssen. Über den Referentenentwurf aus dem Jahr 2022 berichtete die Forschungsstelle Recht bereits im August 2022.[2]

II. Anwendungsbereich

Vom HinSchG erfasst sind nur natürliche Personen, „die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese an die nach diesem Gesetz vorgesehenen Meldestellen melden oder offenlegen (hinweisgebende Personen).“[3] Darunter fallen Arbeitnehmer oder auch Praktikanten, die ein unentgeltliches Praktikum absolvieren. Des Weiteren sind als Beschäftigte u.a. Beamte, Richter, Soldaten, arbeitnehmerähnliche Personen und Menschen, die in Behindertenwerkstätten arbeiten, aufgezählt.[4] Ein Betriebsrat hingegen ist nicht geschützt, da er keine natürliche Person ist. Ein Betriebsratsmitglied hingegen schon.[5] Darüber hinaus werden auch die Personen geschützt, die Gegenstand einer Meldung sind oder von ihr betroffen sind.[6] Die Schutzgüter sind abschließend aufgelistet. So sind gemäß § 2 Abs. 1 Nr. 1 – 10 HinSchG alle strafbewehrten Verstöße erfasst, ebenso wie bußgeldbewehrte Verstöße, soweit sie „dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane“ dienen.[7] Diese Bestimmung ist durchaus weit zu verstehen und umfasst auch die Zahlung eines Entgelts entgegen dem Mindestlohngesetz. Weitere geschützte Güter sind unter anderem die Bekämpfung der Geldwäsche, Vorgaben zur Produktsicherheit, zur Sicherheit

1 Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.

2 Rennert, Die Pfeife tönt zur Nachspielzeit, DFN-Infobrief Recht 8/2022 und Rennert, Meinungsfreiheit verpflichtet, DFN-Infobrief Recht 09/2021.

3 § 1 Abs. 1 HinSchG.

4 § 3 Abs. 8 HinSchG.

5 *Bruns*, NJW 2023, 1610 Rn. 1.

6 § 1 Abs. 2 HinSchG.

7 § 2 Abs. 1 Nr. 1 f. HinSchG.

im (Straßen-, Eisenbahn-, See- und Luft-) Verkehr, Umweltschutz, Lebensmittelsicherheit und der Schutz personenbezogener Daten.[8] Sicherheitsrelevante Bereiche wie Geheimdienste sind jedoch vom Gesetz ausgenommen.[9] Edward Snowden wäre vom HinSchG mithin nicht umfasst.[10] § 5 HinSchG enthält eine Aufzählung von Sicherheitsinteressen sowie Verschwiegenheits- und Geheimhaltungspflichten, die Vorrang genießen. Darunter fallen auch berufsständische Verschwiegenheitspflichten wie die der Rechtsanwälte und Ärzte.[11] Meldungen, die Informationen aus diesen Aufzählungsbereichen enthalten, fallen nicht in den Anwendungsbereich des HinSchG.

Geschäftsgeheimnisse oder Informationen, die einer Verschwiegenheitspflicht durch Vertrag oder Gesetz unterliegen, sind außerdem nur umfasst, wenn hinreichender Grund zu der Annahme besteht, „dass die Weitergabe oder die Offenlegung des Inhalts dieser Informationen notwendig ist, um einen Verstoß aufzudecken“, und hinreichender Grund zu der Annahme besteht, dass (1.) der Verstoß die Gefahr irreversibler Schäden oder eine unmittelbare oder offenkundige Gefährdung des öffentlichen Interesses darstellen kann oder (2.) im Fall einer externen Meldung Repressalien zu befürchten sind oder (3.) Beweismittel unterdrückt oder vernichtet werden könnten oder das Verfahren durch Absprachen oder sonstige Umstände konterkariert werden könnte.[12]

III. Meldestellen

Bei den durch das HinSchG einzurichtenden Meldestellen wird zwischen internen und externen Meldestellen unterschieden. Der Hinweisgeber hat nach § 7 HinSchG ein Wahlrecht, an welche Meldestelle er sich wendet.

1. Interne Meldestellen

Zur Einrichtung einer internen Meldestelle sind Beschäftigungsgeber verpflichtet, die in der Regel 50 Personen beschäftigen.[13] Bei Bund und Ländern bestimmt die oberste Bunds- oder Landesbehörde Organisationseinheiten in Form von einzelnen oder mehreren Behörden, Verwaltungsstellen, Betrieben oder Gerichten. Für Gemeinden und Gemeindeverbände gilt die Pflicht zur Einrichtung und zum Betrieb interner Meldestellen nach Maßgabe des jeweiligen Landesrechts.[14] Für eine jeweilige Organisationseinheit ist dann eine interne Meldestelle einzurichten. Die internen Meldestellen sind in die Lage zu versetzen, ihre Aufgabe wahrnehmen zu können. Dazu zählt das Prüfen von Meldungen und das Ergreifen von Folgemaßnahmen.[15]

Für die Organisationsform gibt es keine konkreten Vorgaben. Mit den Aufgaben der internen Meldestelle kann eine beim Beschäftigungsgeber beschäftigte Person oder auch ein Dritter, etwa eine Rechtsanwaltskanzlei, betraut werden.[16] Mehrere, unabhängig voneinander bestehende private Beschäftigungsgeber mit 50 bis 239 Beschäftigten können eine gemeinsame Stelle einrichten.[17]

Die Meldestellen sind mit unabhängigen und fachlich kompetenten Personen zu besetzen.[18] Sie dürfen neben ihrer Tätigkeit für die interne Meldestelle auch andere Aufgaben und Pflichten wahrnehmen, solange diese nicht zu Interessenkollisionen führen.[19] Wann dies der Fall ist, hat der Gesetzgeber nicht festgelegt.

---

8 Die vollständige Liste enthält § 2 Abs. 3 HinSchG.

9 § 5 HinSchG.

10 Bruns, NJW 2023, 1610 Rn. 10.

11 § 5 Abs. 2 Nr. 3 f. HinSchG.

12 § 6 i.V.m. § 33 Abs. 1 Nr. 2 und 3 HinSchG.

13 § 12 Abs. 1 und 2, § 3 Abs. 8 f. HinSchG.

14 § 12 Abs. 1 HinSchG.

15 § 12 Abs. 4 HinSchG.

16 § 14 Abs. 1 S. 1 HinSchG.

17 § 14 Abs. 2 HinSchG.

18 § 15 Abs. 1 f. HinSchG.

19 § 15 Abs. 1 S. 1 f. HinSchG.

Die zur Einrichtung einer Meldestelle Verpflichteten haben Meldekanäle einzurichten, über die sich Beschäftigte an die internen Meldestellen wenden können. Der Gesetzgeber empfiehlt auch die Bearbeitung anonymer Meldungen, schreibt aber ausdrücklich, dass keine Verpflichtung besteht, anonyme Meldungen durch die Gestaltung der Meldekanäle zu ermöglichen.[20]

Die interne Meldestelle prüft unter anderem eine eingehende Meldung auf ihre Stichhaltigkeit und ergreift angemessene Folgemaßnahmen.[21] Folgemaßnahmen sind beispielsweise interne Untersuchungen, die Abgabe an eine zuständige Behörde oder auch der Abschluss aus Mangel an Beweisen.[22]

2. Externe Meldestellen

Zur Errichtung externer Meldestellen ist der Bund verpflichtet. Sie ist beim Bundesamt für Justiz einzurichten.[23] Außerdem hat der Bund eine weitere externe Meldestelle einzurichten für externe Meldungen, die die externe Meldestelle des Bundes betreffen.[24] Auch die Länder können eigene, dann vorrangige, externe Meldestellen einrichten. Diese sind für Meldungen, die die jeweilige Landesverwaltung und die jeweiligen Kommunalverwaltungen betreffen, zuständig.[25] Auch für Meldungen, die diese Meldestellen betreffen, ist die externe Meldestelle des Bundes zuständig.[26]

Externe Meldestellen sollen unabhängige Beratung und Informationen für potentielle Hinweisgeber bieten. Sie weisen auf die Möglichkeit der internen Meldung hin, schildern den Ablauf des Verfahrens, bieten Beratung über bestehende Abhilfemöglichkeiten und Verfahren für den Schutz vor Repressalien.[27] Das Personal der Meldestellen ist entsprechend zu schulen.[28]

Für die Meldekanäle externer Meldestellen gilt das Gleiche wie für interne Meldestellen. Auch externe Meldestellen sind grundsätzlich nicht zur Bearbeitung anonymer Meldungen verpflichtet.[29] Allerdings können die Länder für ihre fakultativen externen Meldestellen eine Verpflichtung zur Ermöglichung der Abgabe anonymer Meldungen vorsehen.[30] Als Folgemaßnahmen können externe Meldestellen auch Auskünfte von dem betroffenen Beschäftigungsgeber und auch von Behörden verlangen.[31] Dieses Auskunftsverlangen ist innerhalb angemessener Frist zu beantworten.[32]

IV. Meldungen

Die Meldestellen haben die Vertraulichkeit der Identität des Hinweisgebers, der Person, die Gegenstand der Meldung ist, und sonstige in der Meldung genannte Personen zu wahren.[33] Ausnahmen vom Vertraulichkeitsgebot gelten für Hinweisgeber, die vorsätzlich oder grob fahrlässig unrichtige Informationen über Verstöße melden.[34] Außerdem dürfen Informationen, die

---

20 § 16 Abs. 1 HinSchG.

21 § 17 Abs. 1 HinSchG.

22 § 18 HinSchG.

23 § 19 HinSchG.

24 § 23 Abs. 1 HinSchG.

25 § 20 HinSchG.

26 § 23 Abs. 2 HinSchG.

27 § 24 Abs. 1 f. HinSchG.

28 § 25 Abs. 2 HinSchG.

29 § 27 Abs. 1 S. 2 f. HinSchG.

30 § 27 Abs. 1 S. 3 HinSchG.

31 § 29 Abs. 1 S. 1 HinSchG.

32 § 29 Abs. 1 S. 2 HinSchG.

33 § 8 Abs. 1 HinSchG.

34 § 9 Abs. 1 HinSchG.

sich auf die Identität des Hinweisgebers beziehen, aufgrund einer Anordnung im Verwaltungsverfahren oder gerichtlicher Anordnung an Strafverfolgungsbehörden weitergegeben werden. Über die Weitergabe ist der Hinweisgeber vorab zu informieren.[35] Eingehende Meldungen sind von der Meldestelle zu protokollieren und drei Jahre aufzubewahren.[36]

Werden durch den Beschäftigungsgeber anonyme Meldungen zugelassen, sollte sich ein potentieller Hinweisgeber genau überlegen, ob er davon Gebrauch macht. Nachfragen seitens der Meldestelle sind bei einer anonymen Meldung naturgemäß nicht möglich. Auch Verfahrensrechte, wie die Bestätigung des Eingangs und die Rückmeldung zu ergriffenen Folgemaßnahmen, sind dann nicht mehr möglich.

V. Offenlegung

Besonders heikel ist die Offenlegung von Informationen. Hinweisgeber, die Informationen offenlegen, fallen nur unter die Schutzmaßnahmen des HinSchG, wenn sie zuvor eine externe Meldung erstattet haben und hierauf keine geeigneten Folgemaßnahmen innerhalb der Frist für die Rückmeldung ergriffen wurden oder keine Rückmeldung erhalten haben.[37] Ohne vorherige externe Meldung ist die Offenlegung nur in Notfällen zulässig. Das ist der Fall, wenn ein hinreichender Grund zu der Annahme besteht, dass (1.) der Verstoß die Gefahr irreversibler Schäden oder eine unmittelbare oder offenkundige Gefährdung des öffentlichen Interesses darstellen kann oder (2.) im Fall einer externen Meldung Repressalien zu befürchten sind oder (3.) Beweismittel unterdrückt oder vernichtet werden könnten oder das Verfahren durch Absprachen oder sonstige Umstände konterkariert werden könnte.[38] Die Offenlegung setzt mithin die Erfüllung hoher Voraussetzungen voraus.

Ein verstecktes Recht zur Offenlegung bleibt dem Hinweisgeber jedoch: Nach Abschluss des Verfahrens durch eine externe Meldestelle hat der Hinweisgeber die Möglichkeit, Versagungsgegenklage vor dem Verwaltungsgericht zu erheben.[39] Die Klage erfordert weder ein Vorverfahren noch eine Klagebefugnis.[40]

VI. Schutzmaßnahmen

Als Schutzmaßnahmen sieht das Gesetz vor, dass der Hinweisgeber nicht für die Beschaffung von oder den Zugriff auf Informationen verantwortlich gemacht werden kann. Eine Ausnahme besteht, wenn die Beschaffung nicht selbst eine Straftat darstellt.[41]

Gegen den Hinweisgeber gerichtete Repressalien sowie deren Androhung und Versuch sind verboten.[42] Zudem greift eine Beweislastumkehr: Bei einer durch den Hinweisgeber erlittenen Benachteiligung muss der Benachteiligende beweisen, „dass die Benachteiligung auf hinreichend gerechtfertigten Gründen basierte oder nicht auf der Meldung oder Offenlegung beruhte."[43] Bei einem Verstoß gegen das Verbot von Repressalien hat der Hinweisgeber einen verschuldensabhängigen[44] Schadensersatzanspruch.[45] Bei einer vorsätzlichen oder grob fahrlässigen Falschmeldung oder falschen Offenlegung ist jedoch der Hinweisgeber zum Schadensersatz verpflichtet.[46]

35 § 9 Abs. 1 HinSchG.

36 § 11 HinSchG.

37 § 32 Abs. 1 Nr. 1 HinSchG.

38 § 32 Abs. 1 Nr. 2 HinSchG.

39 § 31 Abs. 7 S. 1 HinSchG.

40 *Bruns*, NJW 2023, 1609 Rn. 35.

41 § 35 Abs. 1 HinSchG.

42 § 36 Abs. 1 HinSchG.

43 § 36 Abs. 2 HinSchG.

44 *Bruns*, NJW 2023, 1609 Rn. 42, der von einer Vermutung des Verschuldens nach § 280 Abs. 1 S. 2 BGB ausgeht.

45 § 37 Abs. 1 HinSchG.

46 § 38 HinSchG.

VII. Sanktionen

Das Meldeverfahren und dessen Modalität sind durch diverse Bußgeldvorschriften geschützt. So kann die Behinderung einer Meldung, das Ergreifen einer Repressalie, jeweils deren Versuch oder der Bruch der Vertraulichkeit mit einem Bußgeld bis zu EUR 50.000,00 belegt werden.[47] Das wissentliche Offenlegen einer unrichtigen Information oder die Verhinderung der Einrichtung oder des Betriebs einer Meldestelle kann mit bis zu EUR 20.000,00 geahndet werden.[48]

VIII. Hochschulbezug

Hochschulen können je nach Landesrecht zur Errichtung einer internen Meldestelle verpflichtet sein. Darüber hinaus können sie Adressat eines Auskunftsverlangens einer externen Bundes- oder Landesmeldestelle werden. Beschäftigte an Hochschulen können seit dem 31. Mai 2023 Hinweise an die Meldestelle richten. Üblicherweise veröffentlicht die Hochschule, wie die jeweilige Meldestelle erreicht werden kann.

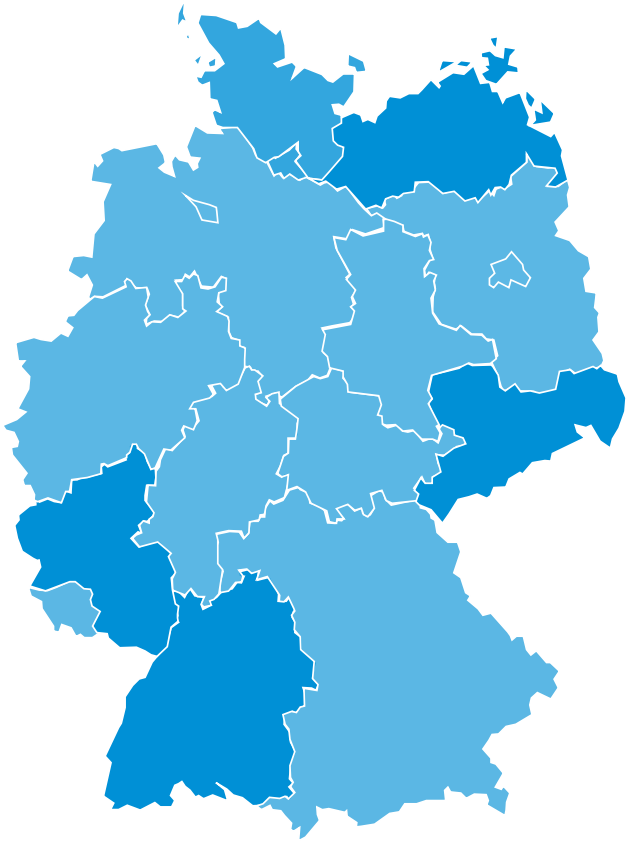

Abbildung 1: Ansiedlung der Meldestellen in den Bundesländern.

Die Karte gibt Aufschluss, ob bei der jeweiligen Hochschule oder dem Ministerium des Bundeslandes eine Meldestelle eingerichtet wurde. Sie bezieht sich nur auf Hochschulen, die in Trägerschaft der Bundesländer stehen (Stand: Juni 2024).

Dunkelblau:
In diesen Bundesländern sind die Meldestellen für den gesamten Organisationsbereich bei den Ministerien angesiedelt: Baden-Württemberg, Mecklenburg-Vorpommern, Rheinland-Pfalz, Sachsen.

Hellblau:
Jede Hochschule hat eine eigene Meldestelle eingerichtet: Bayern, Berlin, Brandenburg, Bremen, Hamburg, Hessen, Niedersachsen, Saarland, Sachsen-Anhalt, Schleswig-Holstein, Thüringen.

Anmerkung zu Bayern: Für Kunsthochschulen ist der Zentrale Dienst der Bayrischen Staatstheater die interne Meldestelle.

Anmerkung zu Hamburg: Die gemeinsame Meldestelle für die HCU, HAW, HFBK, HfMT, TUHH, SUB Hamburg ist bei der TUHH und der HCU Hamburg eingerichtet.

47 § 40 Abs. 2 Nr. 1, 3, Abs. 3, 5 f. HinSchG.

48 § 40 Abs. 1, 2 Nr. 2, Abs. 6 HinSchG.

DFN Infobrief-Recht-Aktuell

- ## Datenschutzrecht: Referentenentwurf des BMDV zum Mobilitätsdatengesetz

  Zweck und Ziel des Referentenentwurfs zum Mobilitätsdatengesetz (MDG) ist es, auf die Bereitstellung einer behördlichen Datengrundlage für die Verkehrsplanung hinzuwirken. Erklärtes Ziel ist dabei auch die Dekarbonisierung und die Ermöglichung neuer Innovationen und Geschäftsmodelle. Der Entwurf enthält Regelungen zur Bereitstellung und Nutzung von Mobilitätsdaten. Mithilfe eines Nationalen Zugangspunktes und eines Bundeskoordinators für Mobilitätsdaten soll ein software-basiertes automatisiertes System die Zusammenarbeit zwischen Datennutzern und Dateninhabern gestalten. Die Eckpunkte zum Mobilitätsdatengesetz wurden bereits im Juli 2023 bekannt. Der Referentenentwurf soll noch dieses Jahr verabschiedet werden, wodurch zukünftig das Mobilitätsniveau im Mobilitätssektor deutlich gesteigert werden könnte.

  Hier erhalten Sie den Link zum Eckpunktepapier und zum Referentenentwurf:
  https://bmdv.bund.de/SharedDocs/DE/Anlage/K/eckpunkte-mobilitaetsdatengesetz.pdf?__blob=publicationFile (zuletzt abgerufen am 23.08.2024).

  https://bmdv.bund.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-20/entwurf-eines-gesetz-bereitstellung-und-nutzung-von-mobilitaetsdaten.pdf?__blob=publicationFile (zuletzt abgerufen am 23.08.2024).

- ## Arbeitsrecht: Verarbeitung von Gesundheitsdaten im Arbeitsverhältnis, Urteil des Bundesarbeitsgerichts vom 20. Juni 2024 – 8 AZR 253/20

  Das Bundesarbeitsgericht entschied, dass die Verarbeitung von Daten durch einen medizinischen Dienst nach Art. 9 Abs. 2 lit. h DSGVO zulässig sein kann. Dieser wurde von der gesetzlichen Krankenkasse mit der Erstellung einer gutachterlichen Stellungnahme zur Beseitigung von Zweifeln an der Arbeitsunfähigkeit des Klägers beauftragt, wobei es sich bei dem Kläger um einen eigenen Arbeitnehmer des Medizinischen Dienstes handelte.

  Hier erhalten Sie den Link zur Pressemitteilung des BAG:
  https://www.bundesarbeitsgericht.de/presse/verarbeitung-von-gesundheitsdaten-im-arbeitsverhaeltnis-medizinischer-dienst-schadenersatz/ (zuletzt abgerufen am 23.08.2024).

- ## Datenschutzrecht/EU-Recht: Lockerung der Voraussetzungen zur Vorratsdatenspeicherung, EuGH 30. April 2024 – C-470/21

  Der EuGH hat die Anforderungen an eine Vorratsdatenspeicherung konkretisiert. Nationale Regelungen sind demnach als Grundlage von Verarbeitungsvorgängen mit dem Unionsrecht (Art. 15 I RL 2002/58 in der Fassung nach RL 2009/136/EG) vereinbar, wenn eine strikte Trennung der IP-Adresse von den übrigen Kategorien personenbezogener Daten (Identitätsdaten, Verkehrsdaten, Standortdaten) vorausgesetzt wird. Es sei dadurch auszuschließen, dass Rückschlüsse auf das Privatleben der betroffenen Person, insbesondere in Form einer Profilbildung gezogen werden können.

  Hier erhalten Sie den Link zur Entscheidung:
  https://curia.europa.eu/juris/document/document.jsf?text=&docid=285361&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1 (zuletzt abgerufen am 23.08.2024).

Kurzbeitrag: Wie geht`s eigentlich Hanna?

Mit der Reform des Wissenschaftszeitvertragsgesetzes sollen die Befristungsregelungen von Wissenschaftler:innen geändert werden

Von Philipp Schöbel, Berlin

Das Bundeskabinett hat im März einen Gesetzesentwurf zur Änderung des Befristungsrechts für die Wissenschaft veröffentlicht. Viele Stimmen kritisieren das Reformvorhaben. Strukturelle Beschäftigungsprobleme von Nachwuchswissenschaftler:innen wird es voraussichtlich nicht lösen.

I. Ziel des Koalitionsvertrags

Ab Sommer 2021 hatten Nachwuchswissenschaftler:innen unter dem Hashtag „#IchBinHanna“ über schwierige Arbeitsbedingungen in Deutschland berichtet und diese scharf kritisiert.[1] In Reaktion darauf hat die Bundesregierung sich im Koalitionsvertrag auf eine Reform des Wissenschaftszeitvertragsgesetzes (WissZeitVG) geeinigt, um verlässliche und sichere Arbeitsbedingungen in der Wissenschaft zu schaffen:[2] Ziel war es, die Planbarkeit und Verbindlichkeit während der Post-Doc Phase deutlich zu erhöhen und frühzeitige „Perspektiven für alternative Karrieren“ zu schaffen. Promotionsstellen sollten die gesamte erwartbare Projektlaufzeit umfassen und mehr wissenschaftliche Dauerstellen für Daueraufgaben entstehen. Insgesamt wollte die Bundesregierung mit diesen Maßnahmen für „eine verbesserte Qualitätssicherung der Promotion“ sorgen. Der nun vorgelegte Gesetzesentwurf[3] setzt diese Ziele nur unzureichend um.

II. Inhalt des Gesetzesentwurfs

Die geplante Novellierung stieß auf breites öffentliches Interesse. Im Vorfeld der Veröffentlichung des Referentenentwurfs des Bundesministeriums für Bildung und Forschung (BMBF) gaben mehr als 80 Interessengruppen Stellungnahmen ab.[4] Die nun geplanten Änderungen betreffen die Befristungsregelungen für Postdocs, Promovierende und studentische Beschäftigte. Erklärte Ziele sind „mehr Verlässlichkeit, Planbarkeit und Transparenz für Wissenschaftlerinnen und Wissenschaftler in frühen Karrierephasen und eine bessere Vereinbarkeit von Beruf und Familie“.

Änderungen für Postdocs:

Die zulässige Befristungsdauer nach der Promotion wird von sechs (bzw. neun in der Medizin) auf vier Jahre für alle Fächer verkürzt. In der Begründung heißt es, dieser Zeitraum sei ausreichend, um zu beurteilen, ob eine Person dauerhaft in der Wissenschaft verbleiben solle. Nach wie vor soll es möglich

1 Tagesschau, Interview, Arbeitsbedingungen an Universitäten – „Menschen- und Wissenschaftsfeindlich“, v. 24.06.2021, abrufbar unter: https://www.tagesschau.de/inland/gesellschaft/ichbinhanna-101.html (zuletzt abgerufen am 11.07.2024).

2 Koalitionsvertrag 2021– 2025 zwischen Der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90 / Die Grünen und den Freien Demokraten (FDP), MEHR FORTSCHRITT WAGEN - BÜNDNIS FÜR FREIHEIT, GERECHTIGKEIT UND NACHHALTIGKEIT, S. 19, abrufbar unter: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf (zuletzt abgerufen am 11.07.2024).

3 Bundesregierung, Entwurf eines Gesetzes zur Änderung des Befristungsrechts für die Wissenschaft, abrufbar unter: https://www.bmbf.de/SharedDocs/Downloads/de/2024/2403_reg_entw_wisszeitvg.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 11.07.2024).

4 Die Mehrzahl der Stellungnahmen ist über die Website des BMBF unter dem Punkt „Gesetz über befristete Arbeitsverträge in der Wissenschaft (WissZeitVG)“ abrufbar unter: https://www.bmbf.de/bmbf/de/service/gesetze/gesetze.html (zuletzt abgerufen am 11.07.2024).

sein, die Befristungsdauer bei Vorliegen einer Behinderung oder für die Betreuung von Kindern pro Kind um zwei Jahre zu verlängern. Künftig soll auch die Betreuung pflegebedürftiger Angehöriger eine Verlängerung rechtfertigen.

Ist die insgesamt zulässige Befristungsdauer ausgeschöpft, soll der Vertrag um weitere zwei Jahre verlängert werden können, wenn sich die/der Arbeitgeber:in verpflichtet hat, den/die Wissenschaftler:in unbefristet zu beschäftigen, falls sie/er bestimmte, in einer Zielvereinbarung niedergeschriebene, wissenschaftliche oder künstlerische Leistungen erbringt.

Änderungen für Promovierende:

Erstverträge sollen künftig regelmäßig eine Laufzeit von mindestens drei Jahren haben. Fachspezifisch und individuell sind damit auch kürzere oder nur geringfügig längere Promotionszeiten als drei Jahre möglich – ohne dass es hierfür einer Begründung bedarf. Bisher gibt es keine Mindestbefristung. Der Gesetzentwurf dokumentiert, dass die durchschnittliche Promotionsdauer laut dem Bundesbericht Wissenschaftlicher Nachwuchs 4,7 Jahre beträgt. Die Mindestlaufzeit von drei Jahren dürfte demnach regelmäßig nicht ausreichen. Der Gesetzesentwurf begründet die Dreijahresfrist damit, dass fachspezifisch und individuell auch kürzere oder nur geringfügig längere Promotionszeiten als drei Jahre möglich seien. Auch für Promovierende soll die Betreuung pflegebedürftiger Angehöriger eine Verlängerung um zwei Jahre rechtfertigen.

Änderungen für SHKs und WHKs:

Für Studierende, die wissenschaftliche oder künstlerische Hilfstätigkeiten (SHKs und WHKs) ausüben, soll die maximale Befristungsdauer künftig von sechs auf acht Jahre erhöht werden. Ziel ist es, den Studierenden mehr Flexibilität zu gewähren. Sie sollen ihre Nebentätigkeit auch nach Überschreiten der Regelstudienzeit neben einem zweiten oder Aufbaustudium fortsetzen können. Insbesondere soll vermieden werden, dass sich studentische Beschäftigte in der Abschlussphase des Studiums eine neue Einkommensquelle suchen müssen.

Außerdem soll für studentische Beschäftigte in der Regel eine Vertragsdauer von mindestens einem Jahr vereinbart werden. Die durchschnittliche Gesamtbeschäftigungsdauer für SHKs und WHKs liegt derzeit jedoch bei rund 20 Monaten. Die Mindestvertragsdauer soll nur in begründeten Fällen unterschritten werden können. Beispiele dafür sind: Betreuung von semesterbegleitenden Tutorien, Tätigkeiten zur Vorbereitung und Durchführung einzelner Veranstaltungen oder eine Beschäftigung im Rahmen zeitlich befristeter Forschungsprojekte im Ausland, zum Beispiel archäologische Grabungskampagnen.

III. Was nicht Inhalt des Gesetzesentwurfs ist

Der Gesetzesentwurf ändert nichts an der Möglichkeit, unbefristete Stellen zu schaffen: Das WissZeitVG lässt das Recht der Hochschulen ausdrücklich unberührt, Wissenschaftler:innen unbefristet anzustellen (§ 1 Abs. 2). Das BMBF sieht es als „Aufgabe der Hochschulen und Forschungseinrichtungen in ihrer Funktion als Arbeitgeber, mehr und in angemessenem Umfang dauerhafte Beschäftigungsverhältnisse zu schaffen.“[5] Es verweist darauf, dass sich grundlegende Strukturen für Nachwuchswissenschaftler:innen bereits geändert hätten. So seien 1.000 neue Professuren mit Tenure-Track[6] geschaffen und die Grundmittel der Hochschulen erhöht worden. Auch außeruniversitären Forschungseinrichtungen hätten sich verpflichtet, attraktive Bedingungen für die gesamte wissenschaftliche Laufbahn zu schaffen.

Der Gesetzesentwurf erkennt, dass die Entscheidung über eine Perspektive für den dauerhaften Verbleib in der Wissenschaft von Faktoren abhängt, „die außerhalb des Befristungsrechts sowie der Kompetenz des Bundes liegen.“ Klarer formuliert: Änderungen im Befristungsrecht lösen die grundsätzlichen

5 BMBF, Die Reform des Wissenschaftszeitvertragsgesetzes, 27.03.2024, abrufbar unter: https://www.bmbf.de/bmbf/shareddocs/faq/wisszeitvg-reform.html (zuletzt abgerufen am 11.07.2024).

6 Bei einer Tenure Track-Professur wird die Person zunächst von einer Universität befristet eingestellt, erhält aber – nach erfolgreicher Bewährungsphase (sog. Tenure Track) – unmittelbar im Anschluss eine dauerhafte Professur: BMBF, Die Tenure-Track-Professur, abrufbar unter: https://www.tenuretrack.de/de/tenure-track-programm/die-tenure-track-professur (zuletzt abgerufen am 11.07.2024).

Probleme der wissenschaftlichen Nachwuchsförderung, wie etwa Teilzeitbezahlung bei Vollzeitarbeit,[7] nicht. Die Länder sind für die Verbesserung der Arbeitsbedingungen in der Wissenschaft zuständig – der Bund kümmert sich lediglich um die Befristung der Arbeitsverträge.

IV. Kritik an den Änderungsplänen

Das „Bündnis gegen Dauerbefristung in der Wissenschaft" – dem unter anderem der Deutsche Gewerkschaftsbund, Verdi sowie die Gesamtbetriebsräte der Fraunhofer- und Max-Planck-Gesellschaften angehören – bezeichnet den Entwurf als „Maximale Enttäuschung nach monatelangem Stillstand".[8] Die vorgeschlagenen Regelungen zu Mindestvertragslaufzeiten für wissenschaftliche Mitarbeiter:innen und studentische Beschäftigte befürwortet es, ansonsten ist es aber der Ansicht, dass der Entwurf „sowohl die Vereinbarkeit von Leben und Beruf als auch die Qualität von Forschung und Lehre massiv" bedrohe.

Kritisch sieht das Bündnis vor allem die geplante Verkürzung der maximalen Befristungsdauer nach der Promotion von sechs auf vier Jahre. Eine pauschale Befristung für die wissenschaftliche Qualifikationsphase sei nach der Promotion nicht mehr sachgerecht. Die mit den kurzen Vertragslaufzeiten einhergehende Pflicht zu ständigen Neubewerbungen verhinderte, dass sich Nachwuchswissenschaftler:innen auf ihre eigene wissenschaftliche Arbeit konzentrieren könnten. Das Bündnis sieht in der Kettenbefristung eine systematische Benachteiligung von Menschen mit Kindern, unsicherem Aufenthaltstitel oder Behinderung.

Das Bündnis hat eine Reihe von Forderungen formuliert. Es fordert, die Mindestlaufzeit für Doktorand:innen regelmäßig auf sechs, mindestens aber auf vier Jahre zu erhöhen. Auch für studentische Beschäftigte soll die Regelvertragslaufzeit auf mindestens zwei Jahre erhöht werden. Nach der Promotion seien eine Übernahme in ein unbefristetes Arbeitsverhältnis oder eine verbindliche Entfristungszusage vorzusehen. Bei familiären Verpflichtungen, Pflege von Angehörigen, Behinderung und chronischer Krankheit soll ein verbindlicher Nachteilsausgleich gewährt werden. Ein weiteres Anliegen ist die Aufhebung der Tarifsperre.[9] Auch wird die Schaffung weiterer unbefristeter Stellen für Daueraufgaben in Lehre und Forschung gefordert. Dieser letzte Punkt kann mit einer Reform des WissZeitVG nicht umgesetzt werden.

---

7 Siehe hierzu: Krempkow/Specht, Leistungsbewertung der Nachwuchsförderung an Hochschulen: Ein Überblick in: Leistungsbewertung in wissenschaftlichen Institutionen und Universitäten. Eine mehrdimensionale Perspektive, S 337, abrufbar unter: https://www.researchgate.net/publication/344172707_Leistungsbewertung_der_Nachwuchsforderung_an_Hochschulen_Ein_Uberblick (zuletzt abgerufen am 26.07.2024).

8 Erklärung des „Bündnis gegen Dauerbefristung in der Wissenschaft" zum unveränderten Referentenentwurf der WissZeitVG-Novelle, 27.03.2024, abrufbar unter: https://www.dgb.de/fileadmin/download_center/Stellungnahmen/Erkl%C3%A4rung_des_%E2%80%9EB%C3%BCndnis_gegen_Dauerbefristung_in_der_Wissenschaft%E2%80%9C_zum_unver%C3%A4nderten_Referentenentwurf_der_WissZeitVG-Novelle.pdf oder https://gesundheit-soziales-bildung.verdi.de/themen/befristung-in-der-wissenschaft/++co++70eb9164-ec12-11ee-8bce-ffa2bee0b3e8 (jeweils zuletzt abgerufen am 11.07.2024).

9 Die Tarifsperre in § 1 Abs. 1 S. 2 WissZeitVG besagt, dass weder zu Gunsten noch zu Ungunsten der Arbeitnehmer:innen von den Vorschriften des WissZeitVG individual- oder tarifvertraglich abgewichen werden darf. In § 1 Abs. 1 S. 3 WissZeitVG ist eine Ausnahme vorgesehen; danach kann durch Tarifvertrag von den Befristungslängen sowie von der Anzahl der zulässigen Verlängerungen befristeter Arbeitsverträge abgewichen werden.

Impressum

Herausgeber

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

Texte:

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der Universität Münster und der Freien Universität Berlin.

Universität Münster
Institut für Informations-,
Telekommunikations- und Medienrecht
-Zivilrechtliche Abteilung-
Prof. Dr. Thomas Hoeren
Leonardo Campus 9, 48149 Münster

Tel. (0251) 83-3863, Fax -38601

E-Mail: recht@dfn.de

Freie Universität Berlin
Professur für Bürgerliches Recht,
Wirtschafts-, Wettbewerbs- und
Immaterialgüterrecht
Prof. Dr. Katharina de la Durantaye, LL. M. (Yale)
Van't-Hoff-Str. 8, 14195 Berlin

Tel. (030) 838-66754

Podcast der Forschungsstelle Recht im DFN

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

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

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