„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

12 / 2024
Dezember 2024

Christkind oder Weihnachtsmann – Wer bringt eigentlich den Datenschutz?
Ein Grundlagenbeitrag zur Datenschutzaufsicht in Deutschland

AI Act – Licht der Europäischen Union?
Die KI-Verordnung der EU ist am 1. August 2024 in Kraft getreten

Süßer die Beschwerden nie klingen
Der Digital Services Act führt ein neues Beschwerdeverfahren vor privaten Schlichtungsstellen ein

Kurzbeitrag: Keine Geschenke vom Bundesarbeitsgericht
BAG zum Ersatz immaterieller Schäden nach unterlassener datenschutzrechtlicher Auskunft

Christkind oder Weihnachtsmann – Wer bringt eigentlich den Datenschutz?

Ein Grundlagenbeitrag zur Datenschutzaufsicht in Deutschland

Von Anna Maria Yang-Jacobi, Berlin

Die Reform des Bundesdatenschutzgesetzes (BDSG) naht. Ein Kernanliegen ist, die Konferenz unabhängiger Datenschutzbehörden des Bundes und der Länder (DSK) als Institution zu stärken. Außerdem sollen Aufsichtsbehörden den Datenschutz effektiver durchsetzen können. Diese Anpassung könnte auch Hochschulen und Forschungseinrichtungen betreffen. Ein Grund, die bisherige Datenschutzaufsicht und die möglichen Neuerungen vorzustellen.

I. Geschichte der datenschutzrechtlichen Regelungen

Spätestens seitdem die europäische Datenschutzgrundverordnung (DSGVO) gilt und sich daraus weitreichende Pflichten ergaben, ist der Datenschutz ein Dauerthema. Dabei ist in Deutschland auf eine über 50-jährige Geschichte zu Regelungen zum Schutz personenbezogener Daten zurückzublicken. Das Land Hessen verabschiedete 1970 das weltweit erste Datenschutzgesetz. 1977 folgte auf Bundesebene erstmalig ein BDSG. Das Bundesverfassungsgericht etablierte im Volkszählungsurteil von 1983[1] das Grundrecht auf informationelle Selbstbestimmung. Der:die Einzelne soll selbst entscheiden können, welche personenbezogenen Daten er:sie preisgeben möchte und wer sie verwenden darf.

Im europäischen Kontext debattierten Interessenvertretende kurze Zeit später über ein europäisches Datenschutzrecht. 1995 verabschiedete der EU-Gesetzgeber die Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-RL). Im weiteren Verlauf kamen Bestimmungen in den europäischen Verträgen hinzu. Mit Inkrafttreten des Vertrags von Lissabon entfaltete unter anderem auch die Charta der Grundrechte der Europäischen Union (GRCh) im Jahr 2009 ihre Wirksamkeit. Die Art. 8 GRCh sowie Art. 16 des Vertrags zur Arbeitsweise der Europäischen Union (AEUV) verankerten den Schutz personenbezogener Daten als europäisches Grundrecht. Aufgrund der zunehmenden Nutzung des Internets und der globalen Bedeutung des Datenverkehrs sollten einheitliche, konkrete Vorgaben zum Schutz personenbezogener Daten folgen. 2016 löste die DSGVO die Datenschutz-RL ab. Nach zweijähriger Übergangszeit gelten die Regelungen zum Datenschutz seit dem 25. Mai 2018 unmittelbar in allen EU-Mitgliedstaaten.

1. Europäische Vorgaben

Als EU-Verordnung sind die Regelungen der DSGVO in allen Mitgliedstaaten direkt anwendbar. Die DSGVO umfasst 99 Artikel. Sie dient dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und dem freien Verkehr dieser Daten. Nach Art. 4 Nr. 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person, also einen Menschen, beziehen. Die verarbeiteten Daten ergeben beziehungsweise ermöglichen eine Identifizierbarkeit eines Menschen. So finden sich in der DSGVO allgemeine Grundsätze zur Verarbeitung von personenbezogenen Daten, zu den Rechten der betroffenen Personen, Pflichten der Verantwortlichen und Auftragsverarbeiter, zur Übermittlung von

1 BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 – Volkszählungsurteil; Das Recht auf informationelle Selbstbestimmung wird vom allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 GG iVm Art. 1 Abs. 1 GG umfasst.

personenbezogenen Daten an Drittländer oder internationale Organisationen, zur Beschaffenheit und Zusammenarbeit der Datenschutzaufsichtsbehörden sowie Rechtsbehelfe und Sanktionsmöglichkeiten. Als zentraler Grundsatz der DSGVO darf eine Verarbeitung personenbezogener Daten nur in Verbindung mit einer Rechtsgrundlage erfolgen.

Für die Datenschutzaufsicht sind Art. 51 und Art. 52 DSGVO von besonderer Bedeutung. Art. 51 Abs. 1 DSGVO stellt fest, dass in jedem Mitgliedstaat eine oder mehrere unabhängige Behörden für die Überwachung der Einhaltung der Vorgaben der DSGVO zuständig sind. Dabei ist es nach Art. 51 Abs. 1, Abs 3 DSGVO ausdrücklich möglich, mehrere Aufsichtsbehörden für den Schutz personenbezogener Daten zu benennen. Die Datenschutzaufsichtsbehörden müssen gemäß Art. 52 DSGVO vollständig unabhängig organisiert sein.

2. Der Datenschutz in Deutschland

Die DSGVO wird also grundsätzlich vor dem nationalen Recht angewendet. Allerdings enthält die DSGVO auch sogenannte Öffnungsklauseln. Über die Öffnungsklauseln können konkrete Bereiche des personenbezogenen Datenschutzes von den Mitgliedstaaten eigenständig spezieller geregelt werden. Das nationale Recht ergänzt und konkretisiert die Regelungen der EU-Verordnung. In der DSGVO sind über 70 Öffnungsklauseln enthalten. Sie sind insbesondere für die Rechtsdurchsetzung und als Rechtsgrundlagen der Datenverarbeitung von Bedeutung. Sofern ein Mitgliedstaat eine nationale Regelung trifft, für die keine Öffnungsklausel in der DSGVO vorgesehen ist, findet die nationale Vorschrift keine Anwendung. Das gleiche gilt, wenn die nationale Regelung der DSGVO widerspricht.

Diese Konkretisierungen und Durchführungsbestimmungen finden sich in Deutschland in einer erneuerten Version des BDSG. Im Einklang mit der DSGVO gilt das BDSG in dieser Form seit dem 25. Mai 2018. Es regelt die nationalen Zuständigkeiten der Behörden, die Behördenstruktur, Rechte der betroffenen Person sowie Pflichten der Verantwortlichen und Auftragsverarbeiter. Zudem enthält das BDSG die deutsche Umsetzung der EU-Datenschutzrichtlinie für Polizei- und Justizbehörden. Diese EU-Richtlinie wird im Gegensatz zu einer Verordnung gerade nicht unmittelbar angewendet, sondern bedarf eines deutschen Umsetzungsgesetzes. Neben dem BDSG bestehen in Deutschland weitere Landesdatenschutzgesetze sowie bereichsspezifische Regelungen zum Datenschutz in Fachgesetzen.

Die Struktur der deutschen Datenschutzaufsicht ist in der EU einzigartig. Kein anderer Mitgliedstaat hat so viele einzelne Datenschutzaufsichtsbehörden. Aufgrund der föderalen Struktur und bereichsspezifischen Gesetze überwachen 41 verschiedene Stellen die Beachtung des Datenschutzes. Zunächst gibt es eine Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI).[2] Die BfDI ist nach § 8 Abs. 1 BDSG eine oberste Bundesbehörde. Als solche arbeitet sie vollkommen unabhängig und untersteht keiner weiteren behördlichen Struktur. Gemäß § 9 Abs. 1 BDSG beaufsichtigt sie die Einhaltung der datenschutzrechtlichen Vorgaben bei öffentlichen Stellen des Bundes sowie Unternehmen, die dem Telekommunikations- und Postdienstsektor angehören. Daneben berät sie die ihr zugeordneten Stellen und Unternehmen. Öffentliche Stellen des Bundes sind Behörden sowie bundesunmittelbare Körperschaften, Anstalten und Stiftungen. Das sind etwa die Bundesministerien, die Bundesagentur für Arbeit, der Bundestag oder auch Berufsgenossenschaften.

Des Weiteren existieren 17 weitere Landesdatenschutzbehörden. Jedes Bundesland hat eine:n eigene:n Landesbeauftragte:n, mit Ausnahme von Bayern, wo zwei Behörden aktiv sind. Die Bundesländer beaufsichtigen die öffentlichen Stellen des Landes sowie nach § 40 Abs. 1 BDSG die nicht-öffentlichen Stellen. Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, also Menschen und private Unternehmen sowie Vereine. Bayern hat diese Zuständigkeit aufgeteilt, sodass der Landesbeauftragte für Datenschutz und Informationsfreiheit für die öffentlichen Stellen des Landes und das Landesamt für Datenschutz für die nicht-öffentlichen Stellen zuständig ist. Auch diese Behörden müssen im Einklang mit einer Entscheidung des Europäischen Gerichtshofs (EuGH) zur behördlichen Gewährleistung des Datenschutzgrundrechts völlig unabhängig handeln können.[3]

2 Seit dem 03.09.2024 wird dieses Amt von der Rechtswissenschaftlerin Prof. Dr. Louisa Specht-Riemenschneider ausgeübt. Zur Neubenennung und den Aufgaben der BfDI siehe Müller, Kurzbeitrag: Neue Wächterin der Daten, DFN-Infobrief Recht 06/2024.

3 EuGH, Urteil vom 09.03.2010 – Rs. C-518/07 – Kommission gegen Deutschland.

Zusätzlich wird der Datenschutz von neun Datenschutzbeauftragten für Religionsgemeinschaften spezifisch beaufsichtigt. Die Aufsicht über den öffentlichen Rundfunk umfasst weitere zwölf eigenständige Datenschutzbeauftragte.

Abschließend spielt die DSK[4] als informelles Gremium eine wichtige Rolle bei der nationalen Rechtsvereinheitlichung. Die DSK besteht aus der BfDI und den 17 Landesdatenschutzbehörden. Das Ziel der DSK ist die Datenschutzgrundrechte zu gewährleisten sowie eine harmonisierte Anwendung des Datenschutzrechts zu ermöglichen und weiterzuentwickeln. Dafür verabschiedet sie Beschlüsse, entwirft gemeinsame Positionspapiere, veröffentlicht Orientierungshilfen oder verfasst Stellungnahmen zu einschlägigen Themen mit Bezug zum Schutz personenbezogener Daten. [5]

II. Aufgaben der Datenschutzbehörden

Zu den Aufgaben der Datenschutzbehörden gehört nicht nur die Aufsicht über den Datenschutz, zusätzlich überwachen die Behörden auch die Gewährleistung der Informationsfreiheit.

1. Datenschutz

Im Bereich des Datenschutzes richten sich die Aufgaben der Datenschutzbehörden zunächst nach der DSGVO. Art. 57 DSGVO zählt 20 Bestimmungen auf. Art. 57 lit. a bis lit. i DSGVO umfassen allgemeine Vorgaben, die sowohl die Durchsetzung der DSGVO als auch eine beratende und informierende Tätigkeit der Behörden aufzeigen. Die weiteren elf Aufgaben sind spezifischer auf einzelne Artikel der DSGVO abgestimmt. Sie gehen von der Erstellung und dem Führen von Listen bis hin zur Einführung und Überwachung von Zertifizierungen und Standardisierungen im Vertragsrecht. § 14 BDSG konkretisiert Art. 57 DSGVO in Bezug auf die deutschen Besonderheiten.

In Zukunft könnte der Arbeitsaufwand der Behörden ansteigen. Die Datenschutzaufsichtsbehörden sollen Teile der neue EU-Rechtsakte zur EU-Datenstrategie durchsetzen. So besagt Art. 37 Abs. 3 des Data Acts (DA) beispielsweise, dass die Datenschutzaufsichtsbehörden auch für die Überwachung der Vorgaben des DA mit Bezug zum Schutz personenbezogener Daten zuständig sind.[6]

2. Informationsfreiheit

Wie an der Namensbezeichnung zu erkennen ist, befassen sich einige Datenschutzaufsichtsbehörden zusätzlich auch mit der Informationsfreiheit. In den Bundesländern, die über ein Informationsfreiheitsgesetz (IFG) verfügen,[7] ist die für den Datenschutz zuständige Person in der Regel auch für die Einhaltung der Informationsfreiheit maßgeblich. Dabei sind die Aufgaben auf den ersten Blick gegensätzlich. Während im Datenschutzrecht der Schutz personenbezogener Daten im Vordergrund steht, dient das Recht auf Informationszugang der Kontrolle und Transparenz von staatlichen Tätigkeiten. Sofern jemand gegenüber einer öffentlichen Stelle Informationen über behördliche Vorgänge verlangt, könnte dieses Verlangen dem Recht auf informationelle Selbstbestimmung bestimmter anderer Personen entgegenstehen, wenn deren Daten in den offengelegten Dokumenten auftauchen. Dieses Spannungsfeld zwischen Datenschutz und Informationsfreiheit müssen die Behörden in Einklang bringen.

Im Rahmen des Datenschutzes verfügen die zuständigen Behörden bereits über praktische Erfahrungen im Bereich der Vermittlung zwischen Bürger:innen und Verwaltung. Die Sicherung der Informationsfreiheit bedarf ähnlicher Anforderungen, sodass die Aufgaben vereint wurden. In der Praxis stehen Datenschutz und Informationsfreiheit nicht im Konflikt. Vielmehr lassen sich beide Funktionen gut miteinander verbinden. Über Schwärzungen bestimmter Passagen mit Personenbezug kann eine Vielzahl an angefragten Dokumenten oder Informationen

4 https://www.datenschutzkonferenz-online.de (zuletzt abgerufen am 17.10.2024).

5 Verschiedene Stellungnahmen der DSK wurden bereits in Beiträgen behandelt: Müller, Künstliche Intelligenz – keine Innovation ohne Diskretion?, DFN-Infobrief Recht 09/2024; Müller, GENehmigte Datennutzung, DFN-Infobrief Recht 07/2024; Müller, Hier werden keine Daten gecloud, DFN-Infobrief Recht 08/2023; Müller, Datenschutz auf Rezept, DFN-Infobrief Recht 02/2023.

6 Zum Data Act siehe Müller, Die Daten sind frei?, DFN-Infobrief Recht 03/2024; Schaller, Data Act: Mehr Daten für alle – check!, DFN-Infobrief Recht 06/2022.

7 Detaillierter zur Informationsfreiheit und den Regelungen der Bundesländer von Bernuth, Die gläserne Universität, DFN-Infobrief Recht 11/2024.

herausgegeben werden. Dem:der Informationsfreiheitsbeauftragten kommt im Vergleich zum Datenschutz mehrheitlich eine vermittelnde Stellung zu. Die Idee ist, ein Umdenken bei den auskunftspflichtigen Stellen herbeizuführen. Dadurch soll die gesetzmäßige Erfüllung von IFG-Anträgen zum Standard werden. Im Rahmen des IFG übt gemäß § 12 Abs. 2 IFG[8] die BfDI diese Rolle aus. Die Verweisung der Aufgaben im Bereich der Informationsfreiheit in § 12 Abs. 3 IFG beziehen sich noch auf die ältere Fassung des BDSG. So sind anlassunabhängige Kontrollen durchzuführen, mögliche Beanstandungen auszusprechen und Tätigkeitsberichte zu erstellen. In den Bundesländern sind die Aufgaben in den landeseigenen Informationsfreiheitsgesetzen ohne Verweisung unmittelbar aufgezählt.[9]

III. Neuerungen durch eine voraussichtliche Reform des BDSG

Im Koalitionsvertrag von SPD, Bündnis 90/Die Grünen und FDP von 2021 strebten die Regierungsparteien eine bessere Durchsetzung und Kohärenz des Datenschutzes an.[10] Zeitgleich evaluierte das Bundesministerium des Inneren und für Heimat (BMI)[11] das BDSG erstmals seit Wirkbeginn im Mai 2018. Aus diesen Überlegungen folgte nach vielen Diskussionen im März 2024 ein Gesetzesentwurf der Bundesregierung zur Änderung des BDSG. [12]

1. Veränderungen durch das BDSG-E

Inhaltlich sind fünf geplante Änderungen von größerer Bedeutung. Interessant ist aus Behördensicht gemäß § 16a BDSG-E die Institutionalisierung der DSK. Gerade in Anbetracht der föderalen Struktur und Vielzahl von Behörden, könnten die Aufsichtsbehörden die Anwendung der DSGVO unterschiedlich handhaben. Bestimmte Handlungen sind zum Beispiel in einem Bundesland ahndungswürdig, während sie in einem anderen Bundesland problemlos erfolgen können. Bisher arbeiten die 18 Datenschutzbehörden von Bund und Ländern in der DSK auf freiwilliger Basis zusammen. Die Institutionalisierung zielt nun darauf ab, schnellere und einheitlichere Beschlüsse zu ermöglichen. Allerdings sollen die Beschlüsse der DSK rechtlich weiterhin unverbindlich bleiben.

§ 4 BDSG-E soll künftig nur die Videoüberwachung öffentlich zugänglicher Räume durch öffentliche Stellen betreffen; die Zulässigkeit einer Videoüberwachung durch nicht-öffentliche Stellen wird abschließend von der DSGVO erfasst. Unter anderem wegen des Scoring-Urteils des EuGH[13] wird § 31 BDSG aufgehoben und soll durch § 37a BDSG-E ersetzt werden. Die Neuregelung des Scorings durch Auskunfteien soll künftig transparenter erfolgen. Eine weitere Änderung könnte auch Hochschulen und Forschungseinrichtungen betreffen.

2. Hochschulen und Forschungseinrichtungen

Auch Hochschulen und Forschungseinrichtungen beschäftigen sich vermehrt mit personenbezogenen Daten. Akademische Forschungsvorhaben können mit besonders sensiblen Daten wie beispielsweise Gesundheitsdaten oder umfangreichen personenbezogenen Daten arbeiten. Für die Verarbeitung dieser Daten bedarf es in der Regel einer Einwilligung. Art. 89 DSGVO enthält zudem eine Öffnungsklausel. Darin werden Garantien und Ausnahmen in Bezug auf die Verarbeitung im öffentlichen Interesse liegender Archivzwecke, wissenschaftlicher oder historischer

8 Ähnliche Regelungen sind in den IFG oder Transparenzgesetzen der Bundesländer zu finden.

9 Als (nicht abschließende) Beispiele: § 18 BerlIFG, § 12 LFIG BW, § 13 BremIFG.

10 Koalitionsvertrag 2021-2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP), S. 14 (SPD-Version) bzw. S. 17 (Die Grünen/FDP-Version).

11 BMI, Evaluierung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, Stand Oktober 2021, https://www.bmi.bund.de/SharedDocs/evaluierung-von-gesetzen/downloads/berichte/evaluierung-bdsg.pdf;jsessionid=584256400099638B04EC5372F327F10C.live861?__blob=publicationFile&v=6 (zuletzt abgerufen am 29.10.2024).

12 Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes vom 27.03.2024, https://dserver.bundestag.de/btd/20/108/2010859.pdf (zuletzt abgerufen am 17.10.2024).

13 EuGH, Urteil vom 7.12.2023 – Rs. C 643/21; Siehe für weitere Informationen Tech, Scoring – Bald nur noch als Entscheidung auf dem Platz?, DFN-Infobrief Recht 6/2023.

Forschungszwecke und statistischer Zwecke ermöglicht. Davon hat der deutsche Gesetzgeber über § 27 BDSG[14] Gebrauch gemacht. Demnach ist die Datenverarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO für wissenschaftliche Forschungszwecke auch ohne Einwilligung möglich, wenn die Verarbeitung erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen. Sofern ausschließlich anonyme Daten verwendet werden, ist die DSGVO nicht anwendbar. Anonym sind Daten allerdings nur, wenn sie nicht einmal mit erreichbarem Zusatzwissen einer identifizierten oder identifizierbaren natürlichen Person zugeordnet werden können.

Im BDSG-E soll das Verfahren der Datenverarbeitung zu wissenschaftlichen Zwecken vereinfacht werden. § 40a BDSG-E enthält eine neue Klarstellung zur zuständigen federführenden Datenschutzaufsichtsbehörde bei gemeinsam verantwortlichen Unternehmen. § 27 Abs. 5 BDSG-E soll dabei auf § 40a BDSG-E verweisen. So soll es Einrichtungen, die Daten zu wissenschaftlichen oder historischen Forschungszwecken oder für statistische Zwecke verarbeiten, bei länderübergreifenden Vorhaben ermöglicht werden, einer einzigen Landesdatenschutzaufsichtsbehörde zu unterstehen. Die Verantwortlichen hätten statt mehrerer Aufsichtsbehörden nur eine einzige Aufsichtsbehörde als Ansprechpartnerin für ihr gemeinsames Datenverarbeitungsvorhaben. Damit tritt der Gesetzgeber einer möglichen Rechtsunsicherheit beim Auftreten unterschiedlicher Rechtsauffassungen mehrerer Aufsichtsbehörden entgegen.

Erwähnenswert ist zuletzt, dass diese besondere Verarbeitungssituation und zukünftig auch die Zuständigkeitsregelung nicht gilt, wenn Hochschulen in ihrer Rolle als Arbeitgeber gefragt sind. Dort ist die DSGVO in ihrer ganzen Fülle anwendbar.

3. Was sich am Gesetzesentwurf mit Blick auf die Datenschutzaufsicht noch ändern könnte

Vor allem die Neuerungen bezüglich der DSK werden stark kritisiert. Dabei geht der Gesetzesentwurf einigen nicht weit genug. Vielmehr sollte die DSK auch eine ständige Geschäftsstelle erhalten, um effizienter arbeiten zu können.[15] Auch die Verbindlichkeit der DSK-Beschlüsse hätte festgelegt werden können. Im Gesetzesentwurf sehen Expert:innen keine große Änderung zum bisherigen Status der DSK.

IV. Ausblick

Eine Beratung des Bundesrats über das neue BDSG hat bereits im März 2024 stattgefunden. Der bisherige Regierungsentwurf wurde im Mai 2024 in erster Lesung im Bundestag beraten. Die Anhörung im zuständigen Ausschuss mit Beteiligung von Expert:innen erfolgte im Juni 2024. Nach dem parlamentarischen Gesetzgebungsverfahren sollten nach den Ausschussberatungen und möglichen Gesetzesänderungen noch die zweite und dritte Lesung im Bundestagsplenum sowie die Schlussabstimmung stattfinden. Wann das neue BDSG allerdings beschlossen und verabschiedet wird, steht noch aus.[16]

Nach Forderungen aus der Wissenschaft soll bis zum Ende des Jahres 2024 zudem noch ein Forschungsdatengesetz[17] vorgestellt werden. Ziel davon ist, den Zugang zu und die Nutzbarkeit von Daten für die wissenschaftliche Forschung zu erleichtern und den Datenschutz forschungsfreundlicher zu gestalten. Außerdem sollen Daten für Forschungszwecke leichter aufzufinden sein.[18] Das Forschungsdatengesetz könnte Hochschulen und Forschungseinrichtungen die Arbeit mit Daten wesentlich erleichtern.

---

14 Die Regelungen des BDSG gelten für öffentliche Stellen des Bundes oder auch private Hochschulen und Forschungseinrichtungen. Für die öffentlichen Hochschulen der Länder sind die Landesdatenschutzgesetze einschlägig. Alle Landesdatenschutzgesetze enthalten eine mit § 27 BDSG vergleichbare Norm, Art. 25 BayDSG, § 25 BbgDSG, § 17 BlnDSG, § 13 BremDSGVOAG, § 13 LDSG BW, § 11 HmbDSG, § 24 HDSIG, § 9 DSG M-V, § 13 NDSG, § 17 DSG NRW, § 22 LDSG RLP, § 12 SächsDSDG, § 27 DSAG LSA, § 23 DSDG, § 13 LDSG SH, § 28 ThürDSG.

15 DSK, Stellungnahme, 12.04.2024, S. 3 ff., https://www.datenschutzkonferenz-online.de/media/st/240412_BDSG-E_Stellungnahme_DSK.pdf (zuletzt abgerufen am 31.10.2024).

16 BMI, Gesetzgebungsverfahren zum Ersten Gesetz zur Änderung des Bundesdatenschutzgesetzes, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/aendg_bdsg.html;jsessionid=C9376A5967210DEC1507C99A5D555173.live892 (zuletzt abgerufen am 17.10.2024).

17 BMBF, Wissenswertes zum Forschungsdatengesetz, https://www.bmbf.de/bmbf/shareddocs/faq/240305_forschungsdatengesetz.html (zuletzt abgerufen am 23.10.2024).

18 BMBF, Eckpunkte BMBF Forschungsdatengesetz, Stand: 28.02.2024 https://www.bmbf.de/SharedDocs/Downloads/de/2024/240306_eckpunktepapier-forschungsdaten.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 23.10.2024).

AI Act – Licht der Europäischen Union?

Die KI-Verordnung der EU ist am 1. August 2024 in Kraft getreten

Von Philipp Schöbel, Berlin

Die europäische KI-Verordnung wird in vielen Bereichen für einen enormen Compliance-Aufwand sorgen. Ein Großteil der Regeln wird auch für Hochschulen und Forschungseinrichtungen eine Rolle spielen.[1]

I. Funktion und Inhalt der KI-Verordnung

Die KI-Verordnung (KI-VO) regelt zum einen den Umgang verschiedener KI-spezifischer Grundrechtsrisiken. Es handelt sich um das Produktsicherheitsrecht. Zum anderen hat sie auch einen innovationsfördernden Teil, der jedoch weitaus kleiner ausfällt.[2] Nachfolgend geht es deswegen um den Umgang mit KI-spezifischen Risiken.

Die Verordnung stellt für verschiedene Akteure eine Reihe von Pflichten auf, wenn sie KI einsetzen oder in Verkehr bringen. Dabei hängen diese Pflichten von der Stellung der einzelnen Akteure in der KI-Wertschöpfungskette ab. Händler haben andere Pflichten als Betreiber oder Anbieter von KI. Es gelten aber nicht für alle Arten von KI die gleichen Pflichten. Die Verordnung unterscheidet zwischen KI-Modellen und KI-Systemen. Für jeden dieser beiden Begriffe gibt es unterschiedliche Risikokategorien wie zum Beispiel verbotene oder hohe Risiken. Abhängig von der Risikokategorie haben die jeweiligen Akteure spezifische Pflichten, die sie einhalten müssen. Die KI-VO verfolgt somit einen risikobasierten Ansatz.

II. Akteure der KI-Wertschöpfungskette

Die KI-VO kennt als zentrale Akteure insbesondere Anbieter und Betreiber. Daneben gibt es Bevollmächtigte, Einführer und Händler. Sonstige Dritte werden an bestimmten Stellen ebenfalls adressiert, um sie den genannten Akteuren gleichzustellen.[3] Die Pflichten für die verschiedenen Akteure gelten grundsätzlich unabhängig davon, ob es sich um eine private oder staatliche Person handelt.

Mit dem Begriff Anbieter ist die Person gemeint, die ein KI-System oder ein KI-Modell entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich.[4] Davon abzugrenzen ist die Rolle des Betreibers, der ein KI-System in eigener Verantwortung verwendet.[5] Daneben gibt es den Einführer, der ein KI-System importiert.[6] Mit dem Begriff des Händlers wird die Person bezeichnet, die ein KI-System auf dem Unionsmarkt bereitstellt und nicht schon Anbieter oder Einführer ist.[7] Zuletzt gibt es Bevollmächtigte, die vom Anbieter dazu bevollmächtigt wurden, in dessen Namen seine Pflichten zu erfüllen.[8]

---

1 Auf einzelne Probleme im Bereich der Lehre wird in einem kommenden Beitrag näher eingegangen.

2 Dazu Schöbel, Europäische Sandkästen für KI, DFN-Infobrief Recht 8/2024, Seite 2.

3 Vgl. etwa Art. 25 Abs. 1 lit. a) KI-VO.

4 Art. 3 Nr. 3 KI-VO.

5 Art. 3 Nr. 4 KI-VO.

6 Art. 3 Nr. 6 KI-VO.

7 Art. 3 Nr. 7 KI-VO.

8 Art. 3 Nr. 5 KI-VO.

In bestimmten Fällen gelten Händler, Einführer, Betreiber oder sonstige Dritte als Anbieter im Sinne der KI-VO. Dies ist der Fall, wenn sie ein bereits in Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-KI-System mit ihrem Namen oder ihrer Handelsmarke versehen, auch wenn vertragliche Vereinbarungen eine andere Aufteilung der Pflichten vorsehen.[9] Zwei weitere Fälle betreffen die Veränderung von KI-Systemen. Wer ein Hochrisiko-KI-System, das bereits in Verkehr gebracht oder in Betrieb genommen wurde, so verändert, dass es weiterhin ein Hochrisiko-KI-System bleibt, gilt ebenfalls als Anbieter.[10] Das Gleiche gilt, wenn ein nicht-hochriskantes KI-System so verändert wird, dass es zu einem Hochrisiko-KI-System wird.[11]

III. Unterscheidung von KI-Systemen und KI-Modellen

Der Begriff des KI-Systems ist in der KI-VO legaldefiniert. Danach handelt es sich bei einem KI-System um ein maschinengestütztes System. Es muss zudem für einen in unterschiedlichem Grad autonomen Betrieb ausgelegt sein. Weiterhin kann es nach seiner Betriebsaufnahme anpassungsfähig sein. Es soll aus erhaltenen Eingaben für explizite oder implizite Ziele ableiten, wie Ausgaben erstellt werden. Ausgaben können zum Beispiel Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen sein, die die physische oder virtuelle Umgebung beeinflussen können.[12]

Ein KI-System im Sinne der KI-VO muss danach vier Merkmale erfüllen:

- autonomer Betrieb,
- Anpassungsfähigkeit,
- Fähigkeit zum Ableiten,
- Ausgaben können die Umgebung beeinflussen.[13]

Autonomie im Sinne der KI-VO meint die Fähigkeit eines KI-Systems, zu einem gewissen Grad unabhängig von menschlichem Zutun zu agieren und ohne menschliches Eingreifen zu arbeiten.[14] Mit dem Begriff der Anpassungsfähigkeit ist die Lernfähigkeit eines KI-Systems gemeint, durch die es sich während seiner Verwendung verändern kann.[15] Die Anpassungsfähigkeit eines KI-Systems kann, muss aber nicht vorliegen.[16] Die Fähigkeit eines KI-Systems abzuleiten, soll über eine einfache Datenverarbeitung hinausgehen und etwa Ansätze maschinellen Lernens sowie logik- und wissensgestützte Konzepte umfassen.[17] Ableiten im Sinne der KI-VO meint, dass das KI-System den Weg vom Input zum Output ableiten muss.[18] Der Output soll die physische oder virtuelle Umgebung beeinflussen können, was den Anwendungsbereich der KI-Definition sehr weit und unbestimmt macht.[19]

Der Begriff des KI-Modells wird hingegen nicht definiert. Nach der Vorstellung des europäischen Gesetzgebers ist ein KI-Modell die Grundlage für ein KI-System und regelmäßig Teil eines solchen, ohne selbst ein KI-System zu sein.[20] Durch das Hinzufügen weiterer Komponenten – etwa einer Nutzerschnittstelle – wird ein KI-Modell zu einem KI-System.[21] Es werden nicht alle KI-Modelle durch die KI-VO geregelt, sondern nur solche mit allgemeinem Verwendungszweck. Bei KI-Modellen mit allgemeinem

9 Art. 25 Abs. 1 lit. a) KI-VO.

10 Art. 25 Abs. 1 lit. b) KI-VO.

11 Art. 25 Abs. 1 lit. c) KI-VO.

12 Art. 3 Nr. 1 KI-VO.

13 Stehen, Ableitungen als wesentliche Fähigkeit von KI-Systemen nach der KI-VO, KIR 2024, 7.

14 Vgl. Erwg. 12 KI-VO.

15 Vgl. Erwg. 12 KI-VO.

16 Wendehorst/Nessler/Aufreiter/Aichinger, Der Begriff des „KI-Systems“ unter der neuen KI-VO, MMR 2024, 605, 608.

17 Vgl. Erwg. 12 KI-VO.

18 Wendehorst/Nessler/Aufreiter/Aichinger, Der Begriff des „KI-Systems“ unter der neuen KI-VO, MMR 2024, 605, 609.

19 Vgl. Wendehorst/Nessler/Aufreiter/Aichinger, Der Begriff des „KI-Systems“ unter der neuen KI-VO, MMR 2024, 605, 608.

20 Vgl. Erwg. 97 KI-VO.

21 Vgl. Erwg. 97 KI-VO.

Verwendungszweck wird unterschieden zwischen solchen mit und ohne systemisches Risiko.[22]

IV. Risikogruppen von KI-Systemen

In der KI-Verordnung sind vier Risikogruppen von KI-Systemen geregelt. Diese umfassen verbotene Praktiken im KI-Bereich, Hochrisiko-KI-Systeme, KI-Systeme mit beschränktem Risiko und KI-Systeme mit minimalem Risiko.[23]

Die KI-VO beinhaltet eine Auflistung von explizit verbotenen Praktiken im Zusammenhang mit KI.[24] Zu den verbotenen KI-Praktiken zählen etwa unterschwellige Beeinflussung, Social Scoring,[25] bestimmte Datenbanken zur Gesichtserkennung[26] und biometrische Kategorisierung.[27] Weiterhin verboten sind das Ausnutzen bestimmter menschlicher Schwachstellen[28] und Profiling im Hinblick auf künftige Straftaten.

Es gibt zwei Arten zur Klassifizierung von Hochrisiko-KI-Systemen: eine produktbezogene und eine anwendungsbezogene.[29] Nach der ersten Art sind solche KI-Systeme hochriskant, die ein Produkt oder ein Sicherheitsbauteil eines Produkts sind, das einer bestimmten Kategorie angehört. Diese Kategorien werden in der KI-Verordnung abschließend aufgeführt. Dazu zählen beispielsweise Sportboote, Medizinprodukte oder Seilbahnen. All diese Produkte müssen einer Konformitätsbewertung durch Dritte unterliegen. Eine Konformitätsbewertung ist ein Verfahren, nach dem vor dem Inverkehrbringen überprüft wird, ob ein Produkt den gesetzlichen Sicherheitsanforderungen entspricht. Teilweise wird gesetzlich festgeschrieben, dass Dritte diese Konformität überprüfen müssen. Bekannte Beispiele für solche Dritte sind etwa die Technischen Überwachungsvereine (TÜV), der Deutsche Kraftfahrzeug-Überwachungsverein (DEKRA) und die Schiffsklassifikationsgesellschaft Germanischer Lloyd.[30] Beispiele für staatliche Stellen sind etwa die Physikalisch-Technische Bundesanstalt (PTB) und die Bundesanstalt für Materialforschung und -prüfung (BAM).[31]

Zudem werden KI-Systeme als Hochrisiko-KI-Systeme eingestuft, wenn sie unter einen in Anhang III der KI-VO genannten Anwendungsfall fallen. Dort sind acht Bereiche aufgeführt (zum Beispiel kritische Infrastruktur, allgemeine und berufliche Bildung sowie Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit). Innerhalb dieser acht Bereiche gibt es verschiedene Anwendungsfälle (auch use-cases genannt). So gibt es etwa im Bereich „4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit“ den Anwendungsfall „KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere um gezielte Stellenanzeigen zu schalten, Bewerbungen zu sichten oder zu filtern und Bewerber zu bewerten“. KI-Systeme sind dann keine Hochrisiko-Systeme, wenn sie zwar in einen der genannten Bereiche fallen, aber kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen bergen.[32]
Die Gruppe der KI-Systeme mit beschränktem Risiko beinhaltet etwa KI-Systeme, die für die direkte Interaktion mit natürlichen

22 Auf die Regelungen zu KI-Modellen mit allgemeinem Verwendungszweck und systemischem Risiko wird in einem kommenden Beitrag genauer eingegangen.

23 Vgl. von Welser: Die KI-Verordnung – ein Überblick über das weltweit erste Regelwerk für künstliche Intelligenz, GRUR-Prax 2024, 485, 486 ff.

24 Art. 5 Abs. 1 KI-VO.

25 Art. 5 Abs. 1 lit. c) KI-VO.

26 Art. 5 Abs. 1 lit. e) KI-VO.

27 von Welser: Die KI-Verordnung – ein Überblick über das weltweit erste Regelwerk für künstliche Intelligenz, GRUR-Prax 2024, 485, 486.

28 Art. 5 Abs. 1 lit. b) KI-VO.

29 Vgl. von Welser: Die KI-Verordnung – ein Überblick über das weltweit erste Regelwerk für künstliche Intelligenz, GRUR-Prax 2024, 485, 486f.

30 Vgl. BMWK, Konformitätsbewertung, abrufbar unter: https://www.bmwk.de/Redaktion/DE/Artikel/Technologie/konformitaetsbewertung.html (zuletzt abgerufen am 07.11.2024).

31 Vgl. BMWK, Konformitätsbewertung, abrufbar unter: https://www.bmwk.de/Redaktion/DE/Artikel/Technologie/konformitaetsbewertung.html (zuletzt abgerufen am 07.11.2024).

32 Art. 6 Abs. 3 KI-VO.

Personen bestimmt sind, sowie solche, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen.[33] Soweit KI-Systeme unter keine der drei dargestellten Risikogruppen fallen, gelten für sie keine gesonderten Anforderungen aus der KI-VO. Es gilt aber die Pflicht zur KI-Kompetenz für Anbieter und Betreiber (dazu unten). In diesem Fall spricht man auch von KI-Systemen mit minimalem Risiko.[34] Davon unberührt bleiben andere gesetzliche Verpflichtungen, etwa Datenschutzvorkehrungen nach der DSGVO.[35]

V. Überblick über die Pflichten

1. KI-Kompetenz

Unabhängig von dem Risiko eines KI-Systems gilt für Anbieter und Betreiber von KI-Systemen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen.[36] KI-Kompetenz meint „die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden."[37] Je nach Kontext, in dem ein KI-System eingesetzt wird, können diese Fähigkeiten, Kenntnisse und Verständnis unterschiedlich sein.[38] Davon umfasst ist etwa das Verständnis der korrekten Anwendung technischer Elemente in der Entwicklungsphase des KI-Systems.[39] Weiter erfordert die KI-Kompetenz die Kenntnis der bei der Verwendung anzuwendenden Maßnahmen und der geeigneten Auslegung der Ausgaben des KI-Systems. Es geht also nicht nur darum, allgemeine KI-Kompetenz zu erwerben, sondern gerade auch um Kompetenzerwerb zu dem KI-System, das eingesetzt wird. Daher können je nach Einsatzbereich unterschiedliche Kenntnisse und Risikobewusstsein nötig sein. Bezüglich eines KI-Systems, das für die Bewertung von Lernergebnissen eingesetzt wird,[40] und eines KI-Systems, das als Sicherheitsbauteil in einem Sportboot verwendet wird,[41] bedarf es jeweils unterschiedlichen Wissens zu Risiken und Funktionsweise.

2. Pflichten für Hochrisiko-KI-Systeme

Die meisten Pflichten gelten für den Umgang mit Hochrisiko-KI-Systemen und insbesondere für die Anbieter von Hochrisiko-KI-Systemen. Sie müssen etwa ein Risiko-[42] und ein Qualitätsmanagementsystem[43] einrichten. Die Einrichtung eines Risikosystems umfasst einen kontinuierlichen iterativen Prozess, der während des gesamten Lebenszyklus eines Hochrisiko-KI-Systems geplant und durchgeführt wird.[44] Dabei müssen Risiken ermittelt werden, die bei der bestimmungsgemäßen Verwendung, bei der Fehlanwendung und auf andere Weise entstehen können.[45] Erfasst sind aber nur solche Risiken, die durch die Entwicklung oder Konzeption des Hochrisiko-KI-Systems oder durch die Bereitstellung ausreichender technischer Informationen

33 Art. 52 Abs. 1,2 KI-VO.

34 Vgl. Möller-Klapperich: Die neue KI-Verordnung der EU, NJ 2024, 337, 441.

35 BfDI, Die KI-Verordnung der EU, abrufbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/KI-Verordnung.html (zuletzt abgerufen am 07.11.2024).

36 Art. 4 KI-VO.

37 Art. 3 Nr. 56 KI-VO.

38 Erwg. 20 KI-VO.

39 Erwg. 20 KI-VO.

40 Vgl. Anhang III Nr. 3 lit b.) KI-VO.

41 Vgl. Anhang I Nr. 3 KI-VO.

42 Art. 16 lit. a) iVm Art. 9 KI-VO.

43 Art. 16 lit. c) iVMmArt. 17 KI-VO.

44 Art. 9 Abs. 2 S. 1 KI-VO.

45 Art. 9 Abs. 2 S. 2 KI-VO.

angemessen gemindert oder behoben werden können.[46] Ein Qualitätsmanagementsystem muss eine Reihe unterschiedlicher Aspekte enthalten; dazu zählen etwa ein Konzept zur Einhaltung der Regulierungsvorschriften sowie Techniken, Verfahren und systematische Maßnahmen für die Entwicklung, Qualitätskontrolle und Qualitätssicherung.[47] Weitere Pflichten betreffen unter anderem die Durchführung eines Konformitätsbewertungsverfahrens,[48] die technische Dokumentation[49] und Anforderungen an die verwendeten Datensätze.[50]

Auch für Betreiber von Hochrisiko-KI-Systemen gilt eine Reihe unterschiedlicher Pflichten. Betreiber müssen Hochrisiko-KI-Systeme entsprechend der beigefügten Betriebsanleitung verwenden.[51] Die Personen, denen die menschliche Aufsicht über ein KI-System übertragen worden ist, müssen über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen.[52] Bevor ein Hochrisiko-KI-System am Arbeitsplatz in Betrieb genommen oder genutzt wird, muss der Arbeitgeber die Arbeitnehmervertretung und die betroffenen Arbeitnehmer:innen über die Nutzung des Hochrisiko-KI-Systems informieren.[53] Die Betreiber müssen den Betrieb des Hochrisiko-KI-Systems anhand der Betriebsanleitung überwachen und gegebenenfalls die Anbieter über auftretende Risiken informieren.[54]

Die Pflichten der Einführer und Händler umfassen vor allem eine abgestufte Kontrolle darüber, ob die KI-Systeme, die sie bereitstellen, die gesetzlichen Anforderungen erfüllen. Händler müssen etwa überprüfen, ob das System mit der erforderlichen CE-Kennzeichnung versehen ist, sowie ob ihm eine Kopie der EU-Konformitätserklärung und Betriebsanleitungen beigefügt sind.[55] Einführer müssen unter anderem überprüfen, ob das Konformitätsbewertungsverfahren vom Anbieter durchgeführt worden ist und ob der Anbieter die technische Dokumentation erstellt hat.[56]

3. KI-Systeme in Interaktion mit Menschen

Anbieter von KI-Systemen, die für die direkte Interaktion mit Menschen bestimmt sind, müssen diese so konzipieren und entwickeln, dass die betroffene Person darüber informiert wird, dass sie mit einer KI interagiert – es sei denn, dass es offensichtlich ist, dass es sich um eine KI handelt.[57] Für Anbieter von KI-Systemen, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen, gilt, dass die Inhalte als KI-generiert gekennzeichnet werden müssen.[58] Betreiber eines KI-Systems, das Deepfakes erstellt, müssen in der Regel offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden.[59] Für künstlerische und satirische Werke gelten Ausnahmeregelungen, um die Darstellung oder den Genuss des Werks nicht zu beeinträchtigen.[60]

---

46 Art. 9 Abs. 3 KI-VO.

47 Art. 17 lit a), c) KI-VO.

48 Art. 16 lit. f) iVm Art. 43 KI-VO.

49 Art. 11 KI-VO.

50 Vgl. Art. 10 KI-VO.

51 Art. 26 Abs. 1 KI-VO.

52 Art. 26 Abs. 2 KI-VO.

53 Art. 26 Abs. 7 KI-VO.

54 Art. 26 Abs. 5 KI-VO.

55 Art. 24 Abs. 1 KI-VO.

56 Art. 23 Abs. 1 KI-VO.

57 Art. 50 Abs. 1 S. 1 KI-VO.

58 Art. 50 Abs. 1 S. 1 KI-VO.

59 Art. 50 Abs. 4 S. 1.

60 Art. 50 Abs. 4 S. 3.

VI. Geltungsbeginn

Regelungen der KI-VO entfalten etappenweise Geltung. Nach Inkrafttreten der KI-VO werden die ersten Regelungen schon ab dem 2. Februar 2025 gelten. Diese ersten Regelungen umfassen verbotene KI-Anwendungen und aber auch die Pflicht für Anbieter und Betreiber von KI, ihren Mitarbeiter:innen KI-Kompetenz zu vermitteln. Eine Reihe weiterer Regelungen gilt ab dem 2. August 2025. Dazu gehören etwa die Regelungen zu KI-Modellen mit allgemeinem Verwendungszweck, die Regeln über die europäischen und nationalen Behörden sowie die Sanktionsregelungen. Die KI-VO wird insgesamt ab dem 2. August 2026 gelten. Die Pflichten für Hochrisiko-KI gelten jedoch erst ab dem 2. August 2027.[61]

VII. KI-VO und Wissenschaft

Für den Bereich der Forschung gibt es in der KI-VO teilweise weitreichende Ausnahmen.[62] Die KI-VO gilt nicht für KI-Systeme und KI-Modelle, die nur für wissenschaftliche Forschung entwickelt und in Betrieb genommen werden.[63] Für die Forschung und Entwicklung von KI gilt die KI-VO ebenfalls nicht, bevor die KI in Verkehr gebracht oder in Betrieb genommen wird – anders ist dies nur für Tests unter Realbedingungen.[64] In den Bereichen Lehre und Hochschulverwaltung gibt es solche Ausnahmen nicht; hier kommt die KI-VO regulär zur Anwendung.

Die KI-VO geht davon aus, dass KI-Systeme in der Bildung eingesetzt werden. Danach sei der „Einsatz von KI-Systemen in der Bildung wichtig, um eine hochwertige digitale allgemeine und berufliche Bildung zu fördern und es allen Lernenden und Lehrkräften zu ermöglichen, die erforderlichen digitalen Fähigkeiten und Kompetenzen – einschließlich Medienkompetenz und kritischem Denken – zu erwerben und auszutauschen, damit sie sich aktiv an Wirtschaft, Gesellschaft und demokratischen Prozessen beteiligen können."[65]

Bestimmte KI-Systeme im Bereich der allgemeinen und beruflichen Bildung werden in der KI-VO als Hochrisiko-KI-Systeme klassifiziert. Die berufliche Bildung meint in diesem Kontext auch die universitäre Bildung, weil berufliche Bildung im Europarecht alle Bildung umfasst, die auf die Vorbereitung des Berufseinstiegs abzielt. Danach sind etwa KI-Systeme, die zur Feststellung des Zugangs oder der Zulassung zu Einrichtungen aller Ebenen der beruflichen Bildung verwendet werden sollen, Hochrisiko-KI-Systeme.[66] Auch solche Systeme, die für die Bewertung von Lernergebnissen verwendet werden sollen, gelten als Hochrisiko-KI.[67]

Ebenfalls als Hochrisiko-KI klassifiziert werden „KI-Systeme, die bestimmungsgemäß zur Überwachung und Erkennung von verbotenem Verhalten von Schülern bei Prüfungen im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung verwendet werden sollen."[68] Hier ist anzumerken, dass damit wahrscheinlich nicht nur Schüler:innen sondern auch Studierende gemeint sind und es sich um ein Redaktionsversehen handelt. Die englische Version der KI-VO spricht von „students" – womit beide Begriffe gemeint sein können. Dafür spricht auch, dass „Schüler" aller Ebenen der allgemeinen und beruflichen Bildung erfasst werden sollen. Für die Anwendung von KI an Hochschulen enthält die KI-VO demnach eine Reihe von Anforderungen, die dem Grundrechtsschutz dienen. In einem kommenden Beitrag sollen die Anforderungen an einzelne KI-Systeme innerhalb der Lehre genauer beleuchtet werden.

---

61 Zu den unterschiedlichen Geltungszeiträumen Art. 113 KI-VO.

62 Dazu bereits Schöbel, DFN-Infobrief Recht 8/2024, Seite 2.

63 Art. 2 Abs. 6 KI-VO.

64 Art. 2 Abs. 8 S. 1, 3 KI-VO.

65 Erwg. 56 KI-VO.

66 Anhang III Nr. 3 lit. a) KI-VO.

67 Anhang III Nr. 3 lit. b) KI-VO.

68 Anhang III Nr. 3 lit. d) KI-VO.

Süßer die Beschwerden nie klingen

Der Digital Services Act führt ein neues Beschwerdeverfahren vor privaten Schlichtungsstellen ein

Von Marc-Philipp Geiselmann, Münster

Seit Geltungsbeginn des Digital Services Acts (DSA) am 17. Februar 2024 haben Personen auch die Möglichkeit, Inhalte auf Online-Plattformen von einer zertifizierten privaten Schlichtungsstelle überprüfen zu lassen. Der Beitrag gibt einen Überblick über die Verfahren und ihre Potenziale.

I. Grundlagen des Digital Services Act[1]

Der DSA ist eine Verordnung der Europäischen Union, die seit dem 17. Februar 2024 vollumfänglich gilt.[2] Die 93 Artikel gliedern sich in fünf Kapitel. Ihnen sind ganze 153 Erwägungsgründe vorangestellt. Ziel der Verordnung ist es, ein sicheres, vorhersehbares und vertrauenswürdiges Online-Umfeld herzustellen.[3] Die Verbreitung rechtswidriger Inhalte soll bekämpft werden.[4] Der Begriff der rechtswidrigen Inhalte ist dabei ein wichtiger Begriff des DSA. Er umfasst alle Informationen, die nicht im Einklang mit dem Unionsrechts oder dem Recht eines Mitgliedstaats stehen.[5] Er umfasst die rechtswidrige Hassrede, terroristische Inhalte, die Weitergabe privater Bilder ohne Zustimmung, den Verkauf gefälschter Produkte, das rechtswidrige Anbieten von Beherbergungsdienstleistungen oder den rechtswidrigen Verkauf von lebenden Tieren.[6] Er ist also sehr weit gefasst.[7] Nicht erfasst sind hingegen Augenzeugenvideos von Verbrechen, dadies zwar eine rechtswidrige Handlung zeigt. Jedoch ist die Verbreitung des Videos nicht rechtswidrig.[8]

Auch nicht vom DSA erfasst sind urheberrechtliche Verstöße, soweit sie durch Unionsvorschriften geregelt sind.[9] Damit bleibt das Urheberrechts-Diensteanbieter-Gesetz (UrhDaG) unberührt, soweit es die DSM-RL[10] umsetzt.[11]

Um rechtswidrige Inhalte zu erfassen, setzt der DSA auch auf die Nutzer der Diensteanbieter. Diese können Inhalte, die sie als rechtswidrig erachten, in verschiedenen Beschwerdeverfahren melden. Meldungen können aber auch von Dritten vorgenommen werden.

---

1 zum DSA auch John, Geschenke verpacken leicht gemacht: Transparenz ist in!, DFN-Infobrief Recht, 12/2023; Rennert, Brüssel reguliert das schon, DFN-Infobrief Recht 6/2022; Gielen, Digital Services Act: Das Plattformgrundgesetz? in DFN-Infobrief Recht 3/2021.

2 Art. 93 Abs. 2 DSA.

3 Art. 1 Abs. 1 DSA.

4 Hofmann F./Raue, in: Hofmann/Raue, DSA, Einleitung Rn. 7.

5 Art. 3 lit. h DSA.

6 ErwG. 12 S. 3 f. DSA.

7 Gerdemann/Spindler, GRUR 2023, 3 (4).

8 ErwG. 12 S. 5 f. DSA.

9 Art. 2 Abs. 4 lit. b DSA.

10 Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG, Abl. EU L 130 vom 17.5.2019 S. 92.

11 Hofmann, in: Hofmann/Raue, DSA, Art. 2 Rn. 46 f.

II. Melde- und Abhilfeverfahren nach Art. 16 f. DSA

Das Melde- Abhilfeverfahren ist von Hostingdiensteanbietern einzurichten. Einen Hostingdiensteanbieter definiert Art. 3 lit. g Ziff. iii DSA als einen Vermittlungsdienst, dessen Leistung darin besteht, von einem Nutzer bereitgestellte Informationen in dessen Auftrag zu speichern. Beispielhaft sind Datenspeicher- und Weitergabedienste, Web-Hostingdienste- Werbeserver und Pastebin-Dienste genannt.[12] Die Größe des betreffenden Anbieters ist unbeachtlich.[13]

1. Berechtigte

Das Beschwerdeverfahren steht ganz allgemein Personen oder Einrichtungen offen. Sie müssen keine Nutzer des Hostingdiensteanbieters sein.[14] Grundsätzlich sind auch anonyme Meldungen zu ermöglichen.[15]

2. Ausgestaltung des Verfahrens

Das Meldeverfahren muss die Meldung rechtswidriger Inhalte ermöglichen.[16] Meldungen, die lediglich gegen die Allgemeinen Geschäftsbedingungen (AGB) eines Hostingdiensteanbieters verstoßen, müssen nicht entgegengenommen werden.[17]

Für das Meldeverfahren sieht der DSA diverse Gestaltungsvorgaben vor. Es muss leicht zugänglich und benutzerfreundlich sein und die Übermittlung von Meldungen ausschließlich auf elektronischem Weg ermöglichen.[18] -Es muss sich ein Meldebutton oder Ähnliches in der Nähe der angezeigten Information befinden.[19] Grundsätzlich bezieht sich die Meldung auf einzelne Inhalte, wobei es möglich sein muss, in einer Meldung mehrere (Einzel-)Inhalte zusammen zu melden.[20]

Das Meldeverfahren muss auch hinreichend genaue und angemessen begründete Meldungen erleichtern.[21] Dazu enthält Art. 16 Abs. 2 DSA eine abschließende Aufzählung bezüglich des Mindestinhalts einer Meldung.[22] Eine Meldung hat eindeutig anzugeben, wo die Verletzung im Internet zu finden ist. Dies kann über eine präzise URL-Adresse geschehen.[23] Wenn die Meldung über ein Kontextmenu in der Nähe der angezeigten Information erfolgt, dann muss die Fundstelle automatisch vorausgefüllt sein. [24]Sie hat außerdem eine hinreichend begründete Erläuterung zu enthalten, die Aufschluss über den Grund der Rechtswidrigkeit gibt.[25] Es ist die Angabe des Namens und der E-Mail-Adresse der meldenden Person zu ermöglichen und schließlich hat die meldende Person eine Erklärung der Richtigkeit und Vollständigkeit abzugeben.[26]

---

12 ErwG. 50 S. 7 DSA, Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 9.

13 ErwG. 50 S. 2 DSA; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 14.

14 Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 16; Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 11; Gerdemann/Spindler, GRUR 2023, 3 (9).

15 ErwG. 50 S. 5 DSA; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 16, 40.

16 Art. 16 Abs. 1 DSA; Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 12; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 20.

17 Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 12; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 20.

18 Art. 16 Abs. 1 S. 2 DSA; Barudi, in: Müller-Terpiz/Köhler, DSA, Art. 16 Rn. 13; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 23.

19 Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 13; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 25.

20 Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 14; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 27.

21 Art. 16 Abs. 2 DSA.

22 Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 16; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 35, 44.

23 Art. 16 Abs. 2 lit. b DSA; ErwG. 53 DSA.

24 Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 37.

25 Art. 16 Abs. 2 lit. a DSA; ErwG. 53 DSA.

26 Art. 16 Abs. 2 lit. c und d DSA; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 39 f.

Auf die Meldung hin, hat der Hostingdiensteanbieter eine Empfangsbestätigung an die meldende Person zu senden, sofern dieser seine E-Mailadresse angegeben hat.[27]

3. Rechtswirkungen einer Meldung

Eine Meldung bewirkt zunächst, dass von einer tatsächlichen Kenntnis oder einem Bewusstsein des Hostingdiensteanbieters bezüglich des gemeldeten Inhalts ausgegangen wird.[28] Voraussetzung dafür ist, dass die Meldung so gefasst ist, dass sie es einem sorgfältig handelnden Anbieter ermöglicht, ohne eingehende rechtliche Prüfung festzustellen, dass der gemeldete Inhalt rechtswidrig ist.[29] Dieser etwas abstrakt anmutende Befund hat weitreichende Folgen: Grundsätzlich sind Hostingdiensteanbieter für die im Auftrag eines Nutzers gespeicherten Informationen von der Haftung befreit.[30] Diese Haftungsprivilegierung entfällt durch eine entsprechende Meldung. Das bedeutet, dass ein Hostingdiensteanbieter, der auf eine Meldung hin nicht handelt, wegen der Verbreitung des gemeldeten Inhalts haftbar ist.[31] Die Haftung beinhaltet sowohl eine strafrechtliche , als auch eine zivilrechtliche Verantwortlichkeit in Form von privaten Schadensersatzansprüchen.[32]

Auch für die Bearbeitung der Meldungen durch den Hostingdiensteanbieter existieren Vorgaben. Über sie ist zeitnah, sorgfältig, frei von Willkür und objektiv zu entscheiden.[33] Eine Anhörung des Nutzers, von dem der Inhalt stammt, ist nicht vorgesehen.[34] Sie könnte sich jedoch aus der Pflicht zur sorgfältigen Bearbeitung ergeben.[35]

Kommt der Hostingdiensteanbieter zu dem Ergebnis, dass der gemeldete Inhalt offensichtlich rechtswidrig ist, hat er diesen zu sperren bzw. zu entfernen.[36] Bei einer Sperrung verhindert der Anbieter, dass Nutzer die Information über seinen Dienst nutzen oder abrufen können.[37] Ein Entfernen ist das endgültige Löschen vom Server des Anbieters.[38] Zur Entscheidungsfindung dürfen auch automatisierte Mittel verwendet werden. Deren Verwendung ist der meldenden Person mitzuteilen.[39]

Schließlich ist die Entscheidung der meldenden Person unverzüglich mitzuteilen. Er ist auf mögliche Rechtsbehelfe gegen diese Entscheidung hinzuweisen.[40] Mit dem Tag der Mitteilung beginnt die sechsmonatige Beschwerdefrist für das interne Beschwerdemanagementsystem.[41] Eine Pflicht zur Begründung der Entscheidung gegenüber der meldenden Person besteht nicht. [42]

Für den Hostingdiensteanbieter ergibt sich keine Pflicht weitere inhaltsgleiche, aber nicht gemeldete, Inhalte zu löschen.[43]

---

27 Art. 16 Abs. 4 DSA.

28 Art. 16 Abs. 3 DSA; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 55 „unwiderlegliche Vermutung".

29 Art. 16 Abs. 3 2. HS DSA.

30 Art. 6 Abs. 1 DSA.

31 Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 26.

32 Hofmann, F., in: Hofmann/Raue, DSA, Art. 6 Rn. 27.

33 Art. 16 Abs. 6 DSA.

34 Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 32; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 62, 89.

35 Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 62.

36 Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 27; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 63, 87, 90.

37 Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 91.

38 Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 92.

39 Art. 16 Abs. 6 S. 2 DSA; Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 38; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 100.

40 Art. 16 Abs. 5 DSA.

41 Art. 20 Abs. 2 DSA; Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 105.

42 Raue, in: Hofmann/Raue, DSA, Art. 16 Rn. 107.

43 Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 34.

Den Nutzern ist eine Begründung der Entscheidung vorzulegen, die darlegt, warum der gemeldete Inhalt rechtswidrig oder nicht mit den Nutzungsbedingungen vereinbar ist. Die Begründungspflicht greift nur für die Fälle, in denen Restriktionen gegen die vom Nutzer bereitgestellten Informationen ergriffen wurden, Beschränkungen von Geldzahlungen vorgenommen wurden, der Dienst dem Nutzer nicht mehr bereit gestellt wird oder das Konto des Nutzers (zeitweise) gesperrt wird.[44] Die Begründung muss die Art der verhängten Restriktion benennen, die Tatsachen und Umstände angeben, auf denen die Entscheidung beruht und auch, ob eine Meldung oder eine eigene Untersuchung Grund für die Entscheidung ist.[45] Außerdem muss auch dem Nutzer gegenüber angegeben werden, ob automatisierte Mittel bei der Entscheidungsfindung verwendet wurden.[46] Dem Nutzer muss die Rechtsgrundlage angegeben werden und eine Begründung dafür, warum die Informationen auf dieser Grundlage als rechtswidrig angesehen werden.[47] Bei einem Verstoß gegen die Nutzungsbedingungen sind die entsprechenden Nutzungsbedingungen mit Begründung anzugeben.[48] Schließlich muss der Nutzer auch über die Rechtsbehelfe informiert werden, die ihm gegen die Entscheidung zustehen, insbesondere das interne Beschwerdemanagementsystem, die außergerichtliche Streitbeilegung und die gerichtlichen Rechtsmittel.[49]

Erhält der Hostingdiensteanbieter Kenntnis von Informationen, die den Verdacht einer Straftat begründen, die eine Gefahr für das Leben oder die Sicherheit einer Person darstellt, so muss er seinen Verdacht unverzüglich den Strafverfolgungs- oder Justizbehörden des jeweiligen Mitgliedstaats mitteilen.[50]

III. Internes Beschwerdemanagementsystem, Art. 20 DSA

Zur Einrichtung eines internen Beschwerdemanagementsystems sind Anbieter von Online-Plattformen verpflichtet.[51] Online-Plattformen sind definiert als ein Unterfall der Hostingdienste, die im Auftrag eines Nutzers Informationen speichern und öffentlich verbreiten.[52] Dabei darf es sich nicht nur um eine unbedeutende Nebenfunktion des Hauptdienstes handeln.[53] Das sind soziale Netzwerke oder Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmen ermöglichen.[54] Suchmaschinen sind keine Online-Plattformen.[55] Von der Pflicht sind Online-Plattformen ausgenommen, die von Kleinst- und Kleinunternehmen betrieben werden.[56]

1. Zweck des internen Beschwerdemanagementsystems

Mittels des internen Beschwerdemanagementsystems müssen sich Nutzer und meldenden Personen oder Einrichtungen gegen Entscheidungen des Anbieters einer Online-Plattform kostenlos und in elektronischer Form wehren können, wenn die Entscheidung damit begründet worden ist, dass es sich bei der Information um rechtswidrige Inhalte handelt oder mit den allgemeinen Geschäftsbedingungen unvereinbar ist.[57] Das gilt für Entscheidungen darüber, ob die Information entfernt oder der Zugang dazu gesperrt oder die Anzeige der Information

44 Art. 17 Abs. 1 DSA.

45 Art. 17 Abs. 1 lit. a und b DSA.

46 Art. 17 Abs. 1 lit. c DSA.

47 Art. 17 Abs. 1 lit. d DSA.

48 Art. 17 Abs. 1 lit. e DSA.

49 Art. 17 Abs. 1 lit. f DSA.

50 Art. 18 Abs. 1 DSA.

51 Art. 20 Abs. 1 DSA; Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 20 Rn. 34; Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 15.

52 Art. 3 lit. i DSA; Hofmann, F., in: Hofmann/Raue, DSA, Art. 3 Rn. 84.

53 Art. 3 lit. i DSA.

54 ErwG. 13 S. 2 DSA.

55 Hofmann, F., in: Hofmann/Raue, DSA, Art. 3 Rn. 83; Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 3 Rn. 86.

56 Art. 19 Abs. 1 DSA.

57 Art. 20 Abs. 1 DSA.

beschränkt wird, die Diensterbringung gegenüber dem Nutzer ausgesetzt oder beendet wird, das Konto des Nutzers ausgesetzt oder geschlossen wird oder Geldzahlungen beendet oder die Möglichkeiten des Nutzers zur Monetarisierung engschränkt wird.[58] Eine meldende Personist beschwerdebefugt, wenn der Anbieter einer Online-Plattform die betreffenden Informationen nicht vollständig löscht oder sperrt.[59] Eine Betroffenheit in eigenen Rechten ist nicht erforderlich.[60]

Es muss meldenden Personen mindestens sechs Monate möglich sein, das Beschwerdemanagement mit der Überprüfung der Entscheidung zu befassen.[61] Die Frist beginnt mit dem Tag, an dem der Nutzer von der Entscheidung in Kenntnis gesetzt wird.[62] Für die Berechnung der Frist gilt die Fristen-VO[63].[64]

2. Ausgestaltung des Verfahrens

Das Beschwerdemanagementsystem muss leicht zugänglich und benutzerfreundlich sein und die Einreichung hinreichend präziser und angemessen begründeter Beschwerden ermöglichen und erleichtern.[65] Dazu muss dem Nutzer in der Regel ein Link zum Beschwerdeformular in der Mitteilung der Entscheidung über die Beschränkung zur Verfügung gestellt werden.[66] Nach Abgabe der Beschwerde ist dem Nutzer ebenfalls eine Empfangsbestätigung zuzusenden.[67]

Die Bearbeitung der Beschwerden hat zeitnah, diskriminierungsfrei, sorgfältig und frei von Willkür zu erfolgen.[68] Auch hier ist keine Anhörung Drittbetroffener vorgesehen.[69] Sie könnte sich wiederum aus der Verpflichtung zur sorgfältigen Bearbeitung ergeben.[70]

Die Entscheidung hat unter der Aufsicht von angemessen qualifiziertem Personal zu erfolgen und nicht allein mit automatisierten Mitteln.[71] Das bedeutet, dass das Aufsichtspersonal über ausreichende juristische Qualifikationen verfügen muss und dass das sonstige Personal hinreichend geschult sein muss.[72] Des Weiteren dürfen bei der Entscheidungsfindung auch automatisierte Mittel eingesetzt werden, wenn auch nicht ausschließlich.[73] Menschliches Personal muss die Entscheidung lediglich überprüfen und nicht eigenständig treffen.[74]

58 Art. 20 Abs. 1 lit. a – d DSA.

59 Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 37.

60 Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 37.

61 Art. 20 Abs. 1 DSA.

62 Art. 20 Abs. 2 DSA.

63 Verordnung (EWG, Euratom) Nr. 1182/71 des Rates vom 3. Juni 1971 zur Festlegung der Regeln für die Fristen, Daten und Termine, Abl. EG Nr. L 124 vom 08.06.1971, S. 1.

64 Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 30.

65 Art. 20 Abs. 3 DSA.

66 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 20 Rn. 55; Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 19.

67 Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 20, 34.

68 Art. 20 Abs. 4 S. 1 DSA.

69 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 20 Rn. 60; Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 58.

70 Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 58; a.A.: Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 20 Rn. 60 „nicht allein aus der Vorgabe zur ‚sorgfältigen' Beschwerdebearbeitung".

71 Art. 20 Abs. 6 DSA.

72 Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 60; etwas weniger strenger Maßstab: Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 20 Rn. 64.

73 Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 61.

74 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 20 Rn. 63; Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 61.

3. Entscheidung und Rechtsfolgen

Der Anbieter der Onlineplattform hat seine Entscheidung in mehreren Fällen unverzüglich rückgängig zu machen. Dabei handelt es sich um Fälle offensichtlicher Unbegründetheit der Beschwerde: Die Beschwerde enthält ausreichende Gründe für die Annahme, dass die Entscheidung, auf eine Meldung hin nicht tätig zu werden, unbegründet ist. Die Informationen, auf die sich die Beschwerde bezieht, sind weder rechtswidrig noch verstoßen sie gegen die allgemeinen Geschäftsbedingungen und die Beschwerde enthält Informationen, aus denen hervorgeht, dass das Verhalten des Beschwerdeführers keine Aussetzung oder Kündigung des Dienstes oder Schließung des Kontos rechtfertigt.[75]

Eine unterlassene Moderation ist unbegründet, wenn den Anbieter der Plattform eine Vornahmepflicht aufgrund eines materiellen Anspruchs trifft oder ein Gesetzesverstoß vorliegt.[76] Auch bei Vorliegen eines AGB-Verstoßes ist eine unterlassene Moderation als unbegründet einzuordnen.[77]

Eine Rücknahmepflicht zugunsten des Nutzers trifft den Anbieter auch, wenn die Beschränkung der Monetarisierung nicht gerechtfertigt ist.[78]

Der Entscheidungsmaßstab wird für die Anbieter von Online-Plattformen eine Gratwanderung, aufgrund der vielen vorzunehmenden rechtlichen Wertungen und Abwägungsentscheidungen.[79] Dem Anbieter steht grundsätzlich ein Einschätzungs- und Entscheidungsspielraum zu.[80] Für die Entscheidungsfällung ist eine überwiegende Wahrscheinlichkeit ausreichend.[81] Zweifel begünstigen aufgrund der Kommunikationsfreiheit den Nutzer.[82]

Die Entscheidung ist dem Beschwerdeführer unverzüglich mitzuteilen und auf die Möglichkeit der außergerichtlichen Streitbeilegung hinzuweisen.[83] Zur Begründung werden keine näheren Ausführungen gemacht. Die Anforderungen, die zur Begründung beim Melde- und Abhilfeverfahren gelten, können vergleichend herangezogen werden.[84]

IV. Außergerichtliche Streitbeilegung, Art. 21 DSA

Gegen Entscheidungen des internen Beschwerdemanagementsystems und des Melde- und Abhilfeverfahrens kann die außergerichtliche Streitbeilegungsstelle angerufen werden.[85] Der maßgebliche Unterschied zu den bisherigen Verfahren besteht darin, dass diese beim Verpflichteten selbst angesiedelt sind, die außergerichtliche Streitbeilegung ist jedoch ein externes gerichtsähnliches Verfahren.[86]

1. Die Streitbeilegungsstelle

Um als außergerichtliche Streitbeilegungsstelle anerkannt zu werden, muss diese vom Koordinator für digitale Dienste des jeweiligen Mitgliedstaats zertifiziert werden.[87] Zum Koordinator

75 Art. 20 Abs. 4 S. 2 DSA.

76 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 20 Rn. 67 f.

77 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 20 Rn. 69 f.

78 Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 66.

79 Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 67.

80 Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 67.

81 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 20 Rn. 76.

82 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 20 Rn. 76.

83 Art. 20 Abs. 5 DSA.

84 Raue, in: Hofmann/Raue, DSA, Art. 20 Rn. 72.

85 Art. 21 Abs. 1 UAbs. 1 DSA; Dregelies, in: Hofmann/Raue, DSA, Art. 21 Rn. 11.

86 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 6.

87 Art. 21 Abs. 3 DSA; Dregelies, in: Hofmann/Raue, DSA, Art. 21 Rn. 67; Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 10.

für digitale Dienste wurde in der Bundesrepublik Deutschland die Bundesnetzagentur bestimmt.[88] Für die Zertifizierung ist es erforderlich, dass die Streitbeilegungsstelle unabhängig, insbesondere finanziell, und unparteiisch ist.[89] Es ist auch erforderlich, dass die Streitbeilegungsstelle die erforderliche Sachkenntnis besitzt, um mögliche rechtswidrige Inhalte oder solche, die den allgemeinen Geschäftsbedingungen der Online-Plattformen widersprechen, als solche beurteilen kann.[90] Ferne muss die Streitbeilegung über elektronische Kommunikationsmittel leicht zugänglich sein und alle erforderlichen Dokumente müssen online eingereicht werden können.[91] Schließlich muss die Streitbeilegungsstelle in der Lage sein, Streitigkeiten rasch, effizient und kostengünstig beizulegen.[92] In der Anforderung Streitigkeiten rasch, effizient und kostengünstig beizulegen, spiegeln sich letztlich die Beweggründe des Gesetzgebers wieder, in diesen Bereichen die Nachteile eines ordentlichen Gerichtsverfahrens zu beseitigen.[93] Eine rasche Bearbeitung konkretisiert der Gesetzgeber dahingehend, dass Streitbeilegungsstellen spätestens nach 90 Tagen, im Falle hochkomplexer Streitfälle nach 180 Tagen, eine Entscheidung zu fällen haben.[94]

Eine Liste der zertifizierten Streitbeilegungsstellen befindet ist auf der Internetseite des digitalen Dienste Koordinators.[95]

2. Verfahrensablauf

Der Gesetzgeber hat kaum Regelungen hinsichtlich des Verfahrensablaufs vorgesehen.[96] Die Streitbeilegungsstellen haben klare und faire Verfahrensregeln aufzustellen, die leicht und öffentlich zugänglich sind.[97] Beide Parteien, also auch die Anbieter von Online-Plattform sind dazu verpflichtet, mit der Streitbeilegungsstelle zusammenzuarbeiten.[98]

Die Streitbeilegungsstellen dürfen für die Einleitung des Verfahrens zur Streitbeilegung vom Nutzer eine Schutzgebühr verlangen.[99] Diese Gebühr soll die Ernsthaftigkeit des Verfahrens garantieren und Missbrauch vorbeugen.[100] Sie wird in Anlehnung an andere Verfahrensvorschriften für Schlichtungsstellen bei höchsten 30,00 EUR liegen.[101]

3. Entscheidung

Die Entscheidung der Streitbeilegungsstelle ist in der Hauptsache nicht bindend.[102] Die europäische Kommission sah im Entwurf des DSA noch eine Bindungswirkung vor, die jedoch auf Initiative der Mitgliedsstaaten geändert wurde.[103] Ein Anbieter einer Online-Plattform ist daher nicht verpflichtet, eine Entscheidung

88 Bernuth, DFN-Infobrief Recht 8/2024, Kurzbeitrag: The floor is yours, Bundesnetzagenur; Pressemitteilung der Bundesregierung vom 14.05.2024, abrufbar unter https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2024/20240514_DSC.html (zuletzt abgerufen am 30.09.2024).

89 Art. 21 Abs. 3 lit. a DSA.

90 Art. 21 Abs. 3 lit. b DSA.

91 Art. 21 Abs. 3 lit. d DSA.

92 Art. 21 Abs. 3 lit. e DSA.

93 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 14.

94 Art. 21 Abs. 4 UAbs. 3 DSA; Dregelies, in: Hofmann/Raue, DSA, Art. 21 Rn. 83, 109 f; Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 34.

95 https://www.dsc.bund.de/DSC/DE/5Streitb/start.html (zuletzt abgerufen am 30.09.2024).

96 Dregelies, in: Hofmann/Raue, DSA, Art. 21 Rn. 104.

97 Art. 21 Abs. 3 lit. f DSA.

98 Art. 21 Abs. 2 UAbs. 1 DSA; Dregelies, in: Hofmann/Raue, DSA, Art. 21 Rn. 105; Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 30.

99 Art. 21 Abs. 5 UAbs. 2 DSA.

100 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 50.

101 Dregelies, in: Hofmann/Raue, DSA, Art. 21 Rn. 116; Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 50 „niedrige ein- oder zweistellige Eurobeträge“.

102 Art. 21 Abs. 2 UAbs. 3 DSA; Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 35, 39.

103 Art. 18 Abs. 1 S. 2 DSA-E; Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 39.

der Streitbeilegungsstelle umzusetzen.[104] Möglich bleibt jedoch, dass diese in der öffentlichen Wahrnehmung eine Prangerwirkung entfalten.[105]

4. Kostentragung

Das Verfahren der außergerichtlichen Streitbeilegung enthält außergewöhnliche Regelungen zur Kostentragung, die den Nutzer, die meldende Person oder Einrichtung begünstigen.[106]

a) Obsiegen des Nutzers
Unterliegt der Anbieter der Online-Plattform, so hat er die Gebühren der Streitbeilegungsstelle zu tragen und dem Nutzer, der meldenden Person oder Einrichtung, alle sonstigen angemessenen Kosten im Zusammenhang mit der Streitbeilegung zu erstatten.[107] Dazu gehört auch die zu zahlende Schutzgebühr. Die angemessenen Kosten können auch die Beauftragung eines Rechtsanwalts für das Verfahren der außergerichtlichen Streitbeilegung umfassen.[108]

b) Obsiegen des Anbieters der Online-Plattform
Im umgekehrten Falle ist der Nutzer, die meldende Person oder die Einrichtung, nicht verpflichtet, Gebühren oder sonstige Kosten zu erstatten, die der Anbieter der Online-Plattform gezahlt hat.[109] Kosten für die Beauftragung eines Rechtsanwalts bekommt der Nutzer im Falle des Unterliegens, ebenso wie die gezahlte Schutzgebühr, nicht ersetzt.[110] Die Privilegierung gilt dann nicht, wenn die Streitbeilegungsstelle zu der Erkenntnis gelangt, dass der Nutzer eindeutig böswillig gehandelt hat.[111]

Durch das Kostenrisiko für den Anbieter der Online-Plattform besteht für diesen ein Interesse, ein möglichst gut funktionierendes Beschwerdemanagement einzurichten.[112]

c) Gebühren
Die von der Streitbeilegungsstelle erhobenen Gebühren müssen angemessen sein und dürfen höchstens kostendeckend für diese sein.[113] Die Berechnungsweise der Gebühren sind vor der Einleitung des Verfahrens zur Streitbeilegung mitzuteilen.[114] Die Gebühren werden meist im dreistelligen Bereich liegen.[115]

V. Vertrauenswürdige Hinweisgeber (trusted flaggers), Art. 22 DSA

Um die Meldung rechtswidriger Inhalte schneller und zuverlässiger zu machen ist vorgesehen, dass es „vertrauenswürdige Hinweisgeber“ gibt.[116] Meldungen, die von vertrauenswürdigen Hinweisgebern in ihrem ausgewiesenen Fachgebiet übermittelt werden, sind von den Anbietern von Online-Plattformen vorrangig zu behandeln und unverzüglich zu bearbeiten.[117] Den Status bekommt eine Stelle vom Koordinator für digitale Dienste zuerkannt, wenn die Stelle über besondere Sachkenntnis und

104 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 42.

105 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 42.

106 Dregelies, in: Hofmann/Raue, DSA, Art. 21 Rn. 112.

107 Art. 21 Abs. 5 S. 1 DSA.

108 Dregelies, in: Hofmann/Raue, DSA, Art. 21 Rn. 119 „grundsätzlich angemessen“; a.A.: Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 55 „regelmäßig nicht“.

109 Art. 21 Abs. 5 S. 2 DSA.

110 Dregelies, in: Hofmann/Raue, DSA, Art. 21 Rn. 120.

111 Art. 21 Abs. 5 S. 2 a.E. DSA.

112 Dregelies, in: Hofmann/Raue, DSA, Art. 21 Rn. 112.

113 Art. 21 Abs. 5 UAbs. 2 DSA.

114 Art. 21 Abs. 5 UAbs. 3 DSA.

115 Dregelies, in: Hofmann/Raue, DSA, Art. 21 Rn. 115; Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 48.

116 ErwG. 61 S. 1 DSA; Nägele/Dilbaz, in: Müller-Terpitz/Köhler, DSA, Art. 22 Rn. 6; Raue, in: Hofmann/Raue, DSA, Art. 22 Rn. 1.

117 Art. 22 Abs. 1 DSA; Raue, in: Hofmann/Raue, DSA, Art. 22 Rn. 1; a.A.: Nägele/Dilbaz, in: Müller-Terpitz/Köhler, DSA, Art. 22 Rn. 18 „nur Anbieter sehr großer Online-Plattformen“.

Kompetenz in Bezug auf die Erkennung, Feststellung und Meldung rechtswidriger Inhalte verfügt.[118] Sie hat außerdem unabhängig von jeglichen Anbietern von Online-Plattformen zu sein und ihre Tätigkeit sorgfältig, genau und objektiv auszufüllen.[119]

Jeder vertrauenswürdige Hinweisgeber hat einmal jährlich einen Bericht über ihre Tätigkeit zu veröffentlichen und dem Koordinator für digitale Dienste zu übermitteln.[120] Sollte ein vertrauenswürdiger Hinweisgeber eine erhebliche Anzahl nicht hinreichend präziser, ungenauer oder unzureichend begründeter Meldungen übermitteln, so kann der Koordinator für digitale Dienste den Status als vertrauenswürdiger Hinweisgeber wieder entziehen. [121]

Eine Liste zugelassener vertrauenswürdiger Hinweisgeber ist auf der Internetseite der Europäischen Kommission verfügbar.[122]

VI. Schadensersatz für Nutzer, Art. 54 DSA

Der DSA sieht für Nutzer einen Schadensersatzanspruch vor.[123] Der Anspruch richtet sich gegen die Anbieter von Vermittlungsdiensten.[124] Haftungsgrund ist ein Verstoß gegen die Verpflichtungen des DSA, was sich insbesondere auf die erläuterten Verfahren bezieht.[125] Voraussetzung für den Anspruch ist, dass gegen eine nutzerbezogene Verpflichtung aus dem DSA verstoßen wurde.[126] Erforderlich ist ferner ein Verschulden des Anbieter, das jedoch vermutet wird.[127] Inhalt des Schadensersatzanspruchs kann auch ein Put-back-Anspruch sein.[128] Löschungen oder Sperrungen müssen dann rückgängig gemacht werden und Beiträge auch inklusive bereits erfolgter Likes, Weiterverlinkungen oder Kommentare zugänglich gemacht werden.[129]

VII. Verhältnis zur gerichtlichen Rechtsdurchsetzung

Die Nutzung der vorgestellten Mechanismen zur Streitbeilegung sind nicht verpflichtend. Es können in sämtlichen Fällen auch ordentliche Gerichte angerufen werden.[130] Während eines Streitbeilegungsverfahrens ist die Verjährung gemäß § 204 Abs. 1 Nr. 4 lit. a BGB gehemmt.[131]

VIII. Fazit und Hochschulbezug

Ob sich die außergerichtliche Streitbeilegung als wirkliche Alternative zur gerichtlichen Streitbeilegung etablieren wird, hängt davon ab, inwieweit sie von Nutzern, meldenden Personen und Einrichtungen angenommen wird.[132] Im besten Falle werden

118 Art. 22 Abs. 2 lit. a DSA.

119 Art. 22 Abs. 2 lit. b und c DSA.

120 Art. 22 Abs. 3 DSA.

121 Art. 22 Abs. 6 f. DSA.

122 https://digital-strategy.ec.europa.eu/de/policies/trusted-flaggers-under-dsa (zuletzt abgerufen am 30.09.2024).

123 Raue, in: Hofmann/Raue, DSA, Art. 54 Rn. 3.

124 Raue, in: Hofmann/Raue, DSA, Art. 54 Rn. 21.

125 Raue, in: Hofmann/Raue, DSA, Art. 54 Rn. 35.

126 Raue, in: Hofmann/Raue, DSA, Art. 54 Rn. 36.

127 Raue, in: Hofmann/Raue, DSA, Art. 54 Rn. 39.

128 Raue, in: Hofmann/Raue, DSA, Art. 54 Rn. 52 f.

129 Raue, in: Hofmann/Raue, DSA, Art. 54 Rn. 53.

130 Dregelies, in: Hofmann/Raue, DSA, Art. 21 Rn. 144.

131 Dregelies, in: Hofmann/Raue, DSA, Art. 21 Rn. 145.

132 Dregelies, in Raue/Hofmann, DSA, Art. 21 Rn. 5.

dadurch staatliche Justizressourcen geschont.[133] Eine hohes Verfahrensaufkommen ist durchaus wahrscheinlich.[134] Allerdings steht insbesondere die außergerichtliche Streitbeilegung auch in der Kritik. So wird die nutzerfreundliche Kostenregelung dazu führen, dass die Streitbeilegungsstellen sich durch die Anbieter finanzieren werden.[135] Dies wird dazu führen, dass sich eine ganze Industrie an Streitbeilegungsstellen um die Anbieter herum bilden wird.[136] Außerdem werden zwar Justizressourcen geschont, aber durch die Streitbeilegungsstellen Doppelstrukturen errichtet.[137]

Angehörige wissenschaftlicher Einrichtungen werden mit den Streitbeilegungsverfahren ebenfalls in Bezug kommen. Sie können als Nutzer künftig Beiträge melden, insbesondere Kommentare, die unter ihre Beiträge platziert werden und rechtswidrige Informationen enthalten können.

Zur Einrichtung eines Melde- und Abhilfeverfahrens nach Art. 16 f. DSA sind Cloud-Angebote der Hochschulen wohl nicht verpflichtet. Cloud-Dienste sind grundsätzlich von der Definition eines Hostingdiensteanbieters erfasst.[138] Art. 6 Abs. 1 DSA beschreibt Hosting jedoch als Dienst der Informationsgesellschaft. Das sind nach Art. 3 lit. a DSA i. V. m. Art. 1 Abs. 1 lit. b der Richtlinie (EU) 2015/1535 gegen Entgelt erbrachte Dienstleistungen. Auch die Literatur listet für Hostingdiensteanbieter beispielhaft ausschließlich kommerzielle Anbieter auf.[139] Die Cloud-Angebote von Hochschulen sind jedoch unentgeltlich erbrachte Dienstleistungen und dürften deshalb vom Anwendungsbereich nicht erfasst sein.

---

133 Dregelies, in Raue/Hofmann, DSA, Art. 21 Rn. 6.

134 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 8, 83.

135 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 57.

136 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 83.

137 Holznagel, in: Müller-Terpitz/Köhler, DSA, Art. 21 Rn. 83.

138 ErwG. 29, S. 4 50 DSA; Gerdemann/Spindler, GRUR 2023, 1 (8); Laude, RDi 2024, 201 Rn. 19 ff; Steinrötter/Schauer, in: Steinrötter, Europäische Plattformregulierung, 1. Auflage 2023, § 2 Rn. 36 – 39.

139 Steinrötter/Schauer, in: Steinrötter, Europäische Plattformregulierung, 1. Auflage 2023, § 2 Rn. 38.

DFN Infobrief-Recht-Aktuell

- ## Datenschutzrecht: Bundesgerichtshofs (BGH) zu Schadensersatzansprüchen nach Scraping-Vorfällen bei Facebook - Leitentscheidungsverfahren

Anfang 2021 wurden personenbezogene Daten von ca. 533 Millionen Facebook-Nutzerinnen und -Nutzern im Internet veröffentlicht. Der BGH hat am 18. November 2024 – VI ZR 10/24 hierzu entschieden, dass ein Schadensersatzanspruch der Betroffenen gegeben sei. Denn nach der Rechtsprechung des Europäischen Gerichtshofs könne auch der bloße und kurzzeitige Verlust der Kontrolle über eigene personenbezogene Daten ein immaterieller Schaden in Sinne der DSGVO sein. Es müsse weder eine konkrete missbräuchliche Verwendung dieser Daten zum Nachteil der Betroffenen erfolgt sein, noch bedürfe es sonstiger zusätzlicher spürbarer negativer Folgen. Der BGH stellte auch eine Ersatzpflicht für künftige Schäden, einen Anspruch auf Unterlassung der Verwendung der Telefonnummer des Geschädigten sowie auf Ersatz der vorgerichtlichen Rechtsanwaltskosten fest.

Hier erhalten Sie den Link zur Pressemitteilung:
https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2024/2024218.html (zuletzt abegerufen am 29.11.2024)

- ## Arbeitsrecht: Betriebsverfassungsrechtlicher Schulungsanspruch – Webinar statt Präsenzschulung?

Das Bundesarbeitsgericht hat am 7. Februar 2024 - 7 ABR 8/23 - entschieden, dass die Übernachtungs- und Verpflegungskosten auch bei bestehender Möglichkeit einer kostengünstigeren Teilnahme per Webinar bei einer Betriebsratsschulung zu erstatten sind.

Hier erhalten Sie den Link zur Pressemitteilung:
https://www.bundesarbeitsgericht.de/presse/betriebsverfassungsrechtlicher-schulungsanspruch-webinar-statt-praesenzschulung/ (zuletzt abegerufen am 29.11.2024)

- ## Sozialrecht: Versicherungsschutz im Homeoffice

Das Bundessozialgericht (BSG) stellte in seiner Entscheidung vom 21. März 2024 – B 2 U 14/21 R klar, dass Versicherte einen Anspruch auf Übernahme von Versicherungskosten durch die Berufsgenossenschaft im Rahmen der Ausübung ihrer Tätigkeit im Homeoffice haben. Bei Ausübung einer Tätigkeit eines selbstständig arbeitenden Busunternehmers kam es zu einem Unfall aufgrund einer defekten häuslichen Heizanlage, wodurch der Versicherte verletzt wurde. Die dadurch anfallenden Kosten wurden gegenüber der Berufsgenossenschaft geltend gemacht, die den Anspruch zunächst ablehnte. Die Revision gegen die vorinstanzliche Entscheidung war schließlich vor dem BSG erfolgreich und das Vorliegen eines Arbeitsunfalls wurde anerkannt.

Hier erhalten Sie den Link zur Entscheidung:
https://www.bsg.bund.de/SharedDocs/Verhandlungen/DE/2024/2024_03_21_B_02_U_14_21_R.html (zuletzt abegerufen am 29.11.2024)

Kurzbeitrag: Keine Geschenke vom Bundesarbeitsgericht

BAG zum Ersatz immaterieller Schäden nach unterlassener datenschutzrechtlicher Auskunft

von Johannes Müller, Münster

Die Frage der Ersatzfähigkeit immaterieller Schäden nach einem Datenschutzverstoß stellt eine der meistdiskutierten Fragen des Datenschutzrechts dar. In der Vergangenheit sind hierzu mehrere wegweisende Urteile ergangen.[1] Das Bundesarbeitsgericht (BAG) hat sich nun in seinem Urteil vom 20. Juni 2024 (Az. 8 AZR 124/23) mit der Frage beschäftigt, ob auch eine nicht erteilte Auskunft nach Art. 15 Datenschutz-Grundverordnung (DSGVO) zum Schadensersatz berechtigt.

I. Der Ersatz immaterieller Schäden nach der DSGVO

Art. 82 DSGVO gibt der betroffenen Person ein Recht zum Schadensersatz, sofern sie aufgrund eines Verstoßes gegen die DSGVO einen Schaden erleidet. Art. 82 Abs. 1 DSGVO erklärt dabei ausdrücklich nicht nur materielle, sondern auch immaterielle Schäden für ersatzfähig. Die schwierige Frage, unter welchen Voraussetzungen immaterielle Schäden ersetzt werden sollen, wurde in Teilen durch den Europäischen Gerichtshof (EuGH) beantwortet. Er hat entschieden, dass grundsätzlich jegliche immateriellen Schäden nach Art. 82 DSGVO ersetzt werden können. Es ist also nicht erforderlich, dass der Schaden erst eine gewisse Erheblichkeitsschwelle überschreiten muss.[2] Als Schäden kommen insbesondere auch reine Gefühlsschäden in Betracht.[3] Gleichzeitig hat der EuGH jedoch auch ausgeführt, dass ein solcher immaterieller Schaden nicht automatisch bei jedem Datenschutzverstoß angenommen werden darf. Stattdessen muss die klagende Partei darlegen, dass ihr tatsächlich ein Schaden entstanden ist.[4] In einem späteren Urteil hat der EuGH zudem entschieden, dass das jeweilige Gericht überprüfen muss, ob der geltend gemachte Schaden tatsächlich begründet erscheint.[5] Ein Verstoß gegen die Vorschriften der DSGVO kann auch darin bestehen, dass der Verantwortliche einem Auskunftsersuchen der betroffenen Person nicht nachkommt. Ob die betroffene Person infolge eines solchen Verstoßes auch Schadensersatz verlangen kann, musste das BAG beantworten.

II. Der Sachverhalt

In dem Fall, der dem Urteil zugrunde lag, befanden sich die Parteien in Gesprächen über die Aufhebung eines Arbeitsverhältnisses, die letztlich erfolglos waren. In diesem Rahmen begehrte die Klägerin und Arbeitnehmerin Auskunft gemäß Art. 15 Abs. 1 DSGVO über die Verarbeitung personenbezogener Daten und eine Kopie der Daten gemäß Art. 15 Abs. 3 DSGVO. Der Arbeitgeber und spätere Beklagte lehnte das Auskunftsbegehren ab.

1 Voget, Kurzbeitrag: Nicht (un)erheblich?!, DFN-Infobrief Recht 07/2023; Müller, Ich glaub, es hackt, DFN-Infobrief Recht 04/2024; Müller, Ist das denn meine Schuld?, DFN-Infobrief Recht 06/2024; Tech, Wer den Scha-den hat, braucht für den Ärger nicht zu sorgen, DFN-Infobrief Recht 08/2024.

2 Voget, Kurzbeitrag: Nicht (un)erheblich?!, DFN-Infobrief Recht 07/2023.

3 Müller, Ich glaub, es hackt, DFN-Infobrief Recht 04/2024.

4 Voget, Kurzbeitrag: Nicht (un)erheblich?!, DFN-Infobrief Recht 07/2023.

5 Müller, Ich glaub, es hackt, DFN-Infobrief Recht 04/2024.

Nachdem das Arbeitsverhältnis durch Kündigung beendet wurde, hat die Klägerin versucht, vor Gericht die Erfüllung des Auskunftsanspruchs zu erzwingen. Gleichzeitig verlangte sie 5.000 Euro Schadensersatz für die unterbliebene Auskunft. Aufgrund der verweigerten Auskunft habe sie keine Möglichkeit zur Überprüfung der Datenverarbeitung gehabt. Sie bezeichnete den Kontrollverlust aufgrund der ihrer Ansicht nach vorsätzlichen und böswilligen Verweigerung als vorsätzlich und böswillig. Im gerichtlichen Verfahren erteilte der Arbeitgeber dann auch Auskunft über die Datenverarbeitung.

Das Arbeitsgericht hat zunächst einen Schadensersatzanspruch in Höhe von 4.000 Euro anerkannt. Das Landesarbeitsgericht hat nach Berufung des Arbeitgebers das Urteil abgeändert und die Klage auf Schadensersatz abgewiesen. Hiergegen hat die Klägerin Revision eingelegt, sodass nun das Bundesarbeitsgericht über die Frage entscheiden musste.

III. Die Entscheidung des BAG

Das BAG hat das Bestehen eines immateriellen Schadens im Sinne von Art. 82 DSGVO abgelehnt. Hierbei berief es sich auf die Rechtsprechung des EuGH. Es erkannte an, dass grundsätzlich auch Gefühlsschäden wie die Angst vor Datenmissbrauch einen Schaden darstellen können und hier-für keine Bagatellgrenze besteht. Das BAG betonte aber, dass ein eigenständiger Schaden festgestellt werden muss, der nicht allein auf die Verletzung einer DSGVO-Vorschrift gestützt werden kann. Die bloße Äußerung entsprechender Befürchtungen reiche alleine nicht aus. Das hypothetische und nicht tatsächliche Risiko einer missbräuchlichen Datenverwendung führe alleine nicht zu einem Schadensersatzanspruch. Stattdessen müsse das Gericht die objektive Plausibilität des behaupteten Schadens überprüfen. In dem Prozess habe die Partei zum Ausdruck ge-bracht, dass ihre Unkenntnis der Datenverarbeitung zu Sorgen führen würde. Nach Auffassung des BAG rufe aber die Nichterfüllung des Auskunftsanspruchs stets Sorgen dieser Art hervor. Sofern man diese Sorgen für einen Schadensersatzanspruch genügen lasse, wäre ein solcher Anspruch stets in Folge eines Verstoßes gegen Art. 15 DSGVO begründet. Damit käme dem Schadenserfordernis keine eigenständige Bedeutung mehr zu. Dies sei nicht mit dem Normverständnis des EuGH[6] und dem nationalen Prozessrecht vereinbar, welche die eigenständige Darlegung eines Schadens erforderten.

IV. Bedeutung für wissenschaftliche Einrichtungen

Auch wissenschaftliche Einrichtungen sehen sich regelmäßig Auskunftsersuchen nach Art. 15 DSGVO ausgesetzt. Diesen sollten sie auch nachkommen, um nicht gegen die DSGVO zu verstoßen. Sofern es dennoch zu einem Rechtsstreit kommt, ist die höchstinstanzliche Auffassung des BAG relevant, nach der allein die typischen Sorgen, die stets mit einer Nichterfüllung des Auskunftsanspruchs einhergehen, keinen relevanten Schaden im Sinne von Art. 82 DSGVO darstellen.

6 Dieses Verständnis des EuGH wird besonders deutlich in der Entscheidung Österreich Post (Az. C-300/21) Rn. 28 ff.; hierzu Voget, Kurzbeitrag: Nicht (un)erheblich?!, DFN- Infobrief Recht 07/2023.

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