„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

3 / 2025
März 2025

Im Maschinenraum einer Online-Plattform

Der Digital Services Act enthält zwei neue Datenzugangsrechte, um sehr große Online-Plattformen und Suchmaschinen zu erforschen

Von Nikolaus von Bernuth, Berlin

Online-Plattformen und Suchmaschinen bestimmen unsere Nutzung des Internets. Ihre Algorithmen und Empfehlungssysteme geben maßgeblich vor, welche Inhalte wem angezeigt werden und welche Informationen wir aufnehmen. Der Digital Services Act sieht unter anderem vor, dass die sehr großen Dienste ausgehende systemische Risiken analysieren und mindern. Um diese Risiken und ihre Ursachen besser zu verstehen, hat die Forschung weitreichende Datenzugangsrechte erhalten. So soll die Wissenschaft zum Verständnis dieser systemischen Risiken beitragen. Ein erster Gerichtsbeschluss stärkt der Forschung den Rücken.

I. Verständnis der großen Plattformen

Der Digital Services Act (DSA) wurde bereits in einer Vielzahl von Beiträgen aus unterschiedlichem Blickwinkel beleuchtet.[1] Die Verordnung hat einen neuen Rechtsrahmen für digitale Vermittlungsdienste geschaffen, sie soll das Internet sicher, vorhersehbar und vertrauenswürdig machen (Art. 1 Abs. 1 DSA). Ein wichtiges Ziel des DSA ist es daher, die Funktionsweise und die Gefahren insbesondere der sehr großen Online-Plattformen und Suchmaschinen besser zu verstehen.

In einem vorigen Beitrag wurden die Pflichten dieser sehr großen Dienste zur Erkennung und Bekämpfung systemischer Risiken vorgestellt.[2] Systemische Risiken nach Art. 34, 35 DSA sind strukturelle Gefahren, die über den Einzelfall hinausreichen, die wir auf sehr großen Online-Plattformen und Suchmaschinen beobachten können. Die Dienste müssen etwa die Verbreitung rechtswidriger Inhalte, Auswirkungen auf Wahlen oder geschlechtsspezifische Gewalt laufend untersuchen. Sollten sie systemische Risiken feststellen, müssen sie Änderungen an ihren Algorithmen, Moderationssystemen oder anderen Funktionalitäten vornehmen, um diese Risiken zu mindern.

An diese Pflichten knüpft eine weitere Norm an, bei der es sich um die für die Wissenschaft wohl wichtigste Vorschrift des DSA handelt. Art. 40 DSA enthält zwei Datenzugangsrechte für Forschende, die es zum Ziel haben, die systemischen Risiken auf Online-Plattformen zu untersuchen und zu verstehen. So wird nicht nur den Plattformen selbst überlassen, die von ihren Diensten ausgehenden Risiken einzuschätzen. Außerdem soll die Position der Wissenschaft gegenüber den Online-Plattformen gestärkt werden.[3] Dieser Beitrag stellt die beiden Datenzugangsrechte im Detail vor.

II. Der volle Datenzugang

Das erste und zugleich bedeutsamste Datenzugangsrecht für Forschende findet sich in Art. 40 Abs. 4 DSA. Dieses Zugangsrecht ermöglicht den Zugang zu allen Daten der sehr großen

1 Zum DSA: John, Geschenke verpacken leicht gemacht: Transparenz ist in!, DFN-Infobrief Recht 12/2023; von Bernuth, Forschung? Unerwünscht., DFN-Infobrief Recht 02/25; Geiselmann, Süßer die Beschwerden nie klingen, DFN-Infobrief Recht 12/2024; von Bernuth, Systemische Risiken riesiger Systeme, DFN-Infobrief Recht 09/2024; von Bernuth, Kurzbeitrag: The floor is yours, Bundesnetzagentur, DFN-Infobrief Recht 08/2024.

2 von Bernuth, Systemische Risiken riesiger Systeme, DFN-Infobrief Recht 09/2024.

3 Zum bislang prekären Rollenverhältnis von Bernuth, Forschung? Unerwünscht., DFN-Infobrief Recht 02/25.

Online-Plattformen oder Suchmaschinen, die für das eigene Forschungsvorhaben nötig sind. Erfasst sind also auch Daten hinter der Nutzungsoberfläche, die nicht sichtbar sind. Dies können etwa Informationen dazu sein, wie oft Inhalte gesehen wurden, wie lange sie angesehen wurden und mit welchen Schlagworten sie im internen Algorithmus eingeordnet werden. Um diesen Datenzugang zu erhalten, müssen Forschende allerdings eine Reihe von Voraussetzungen erfüllen.

1. Wer untersucht werden soll

Verpflichtet zur Bereitstellung des Datenzugangs nach Art. 40 DSA sind sehr große Online-Plattformen und Online-Suchmaschinen. Dazu gehören nach Art. 33 DSA alle Dienste mit mehr als 45 Mio. monatlich aktiven Nutzenden, die explizit als solche benannt wurden.[4] Alle namhaften größeren sozialen Netzwerke (Facebook, X) und Suchmaschinen (Google Search, Bing) fallen in diese Kategorie, aber auch Online-Marktplätze (Amazon, Shein), Videoplattformen (Youtube, Pornhub), App Stores (Apple App Store, Google Play Store) und Enzyklopädien wie Wikipedia.

2. Wissenschaftliche Forschung

Berechtigt zum Zugang nach Art. 40 Abs. 4 DSA sind zugelassene Forschende. Wer diesen Status zuerkannt bekommen möchte, muss die Voraussetzungen in Art. 40 Abs. 8 DSA erfüllen und beim Antrag nachweisen. Erste Voraussetzung ist, dass die Person an eine Forschungseinrichtung im Sinne von Art. 2 Nr. 1 DSM-Richtlinie angeschlossen ist.[5] Hierzu zählen Hochschulen, Institute und ähnliche Einrichtungen, deren vorrangiges Ziel die wissenschaftliche Forschungs- oder Lehrtätigkeit ist.

Der Begriff der „Forschungseinrichtung" nach der DSM-Richtlinie erfasst auch zivilgesellschaftliche Organisationen, solange wissenschaftliche Tätigkeit vorrangiges Ziel ist und keine Gewinne erzielt werden, die nicht wieder in die Forschung fließen. Obwohl Art. 40 Abs. 4 DSA also (im Gegensatz zu Abs. 12) gemeinnützige Organisationen nicht explizit erwähnt, sollen diese ebenfalls zum vollen Datenzugang nach Art. 40 Abs. 4 DSA berechtigt sein. Erwägungsgrund 97 zum DSA stellt dies ebenfalls klar.

Wer an einer Hochschule oder Forschungseinrichtung arbeitet, wird diese Voraussetzungen ohne Probleme erfüllen können. Ohne institutionelle Anbindung kommt ein Datenzugang nach Art. 40 Abs. 12 DSA dagegen nicht in Betracht.

3. Unabhängigkeit und Datensicherheit

Nächste Voraussetzung nach Art. 40 Abs. 8 DSA ist die Unabhängigkeit von kommerziellen Interessen und die Transparenz der Finanzierung des Forschungsvorhabens. Dies könnte immer dann problematisch werden, wenn etwa mit Drittmitteln von kommerziellen Unternehmen gearbeitet wird oder sonstige persönliche Verbindungen zu kommerziellen Akteuren bestehen. Hier zeigt sich das sogenannte Altruismusgebot: Die Forschung muss dem Erkenntnisgewinn dienen, nicht kommerziellen Interessen. Dementsprechend müssen sich die Forschenden auch verpflichten, ihre Ergebnisse kostenfrei zu veröffentlichen.

Wichtig ist zudem, dass die antragstellenden Forschenden nachweisen können, dass sie die Anforderungen an die Vertraulichkeit und Sicherheit der erhaltenen Daten gewährleisten können. Hierzu sollen sie die angemessenen technischen und organisatorischen Maßnahmen, die sie hierzu ergriffen haben, beschreiben. Die Modalitäten dieser infrastrukturellen Bedingungen könnten eine der größten Hürden im Rahmen des Art. 40 Abs. 4 DSA werden. Im Extremfall könnten die Plattformen darauf bestehen, dass auf die Daten nur in speziellen Räumlichkeiten („secure processing environments"),[6] etwa an der Niederlassung des Unternehmens in Irland, zugegriffen werden kann und kein Datentransfer stattfindet. Dies wiederum würde die Rahmenbedingungen des Datenzugangs erheblich unattraktiver machen. Datenforschende plädieren daher dafür, dass secure processing environments nur das letzte Mittel sein dürften,

4 Eine aktuelle Liste findet sich hier: https://digital-strategy.ec.europa.eu/de/policies/list-designated-vlops-and-vloses (alle Links dieses Beitrags zuletzt abgerufen am 15.02.2025).

5 RL (EU) 2019/790.

6 Selinger/Klinger/Ohme, Tech Policy Press, https://www.techpolicy.press/non-public-data-access-for-researchers-challenges-in-the-draft-delegated-act-of-the-digital-services-act/.

wenn andere Lösungen schlicht nicht praktikabel sind.[7] Im Umkehrschluss zeigt sich: Forschende sollten in die Lage versetzt werden, überzeugende Lösungen für die Datensicherheit und Vertraulichkeit glaubhaft machen zu können. Dies erfordert eine gute technische Ausstattung.

4. Erforschung systemischer Risiken

Wie bereits eingangs verdeutlicht, dienen die Datenzugangsrechte dem besseren Verständnis systemischer Risiken der sehr großen Online-Plattformen. Entsprechend verlangt Art. 40 Abs. 8 DSA, dass das Forschungsvorhaben nachweislich auf diese Zwecke abzielt. Darüber hinaus muss plausibel sein, dass die angefragten Daten für das konkrete Forschungsziel tatsächlich erforderlich sind und der Zugang auch nur so lange wie nötig beantragt wird. Hieraus ergibt sich, dass das Forschungsvorhaben bereits bei der Antragstellung recht genau beschrieben und plausibilisiert werden muss. Einen allgemeinen Datenzugang mit der Möglichkeit, das Vorhaben erst anhand der vorgefundenen Daten zu konkretisieren, gibt es somit nicht.

5. Verfahren

Sind all diese Voraussetzungen erfüllt, kann der Datenzugang beantragt werden. Allerdings nicht bei der Online-Plattform oder Suchmaschine selbst: Der Antrag muss beim nationalen Koordinator für digitale Dienste eingereicht werden. Dies ist die mitgliedstaatliche Behörde, die die zentrale Steuerung der Durchsetzung des DSA übernimmt. In Deutschland ist dies eine Koordinationsstelle bei der Bundesnetzagentur, § 14 Abs. 1 Digitale-Dienste-Gesetz (DDG).[8] Nach Art. 40 Abs. 9 DSA prüft die Bundesnetzagentur den eingegangenen Antrag vorab. Sie leitet ihn daraufhin an den Koordinator des Mitgliedsstaats weiter, in dem die Online-Plattform oder Suchmaschine ihre Niederlassung hat (regelmäßig Irland). Der dortige Koordinator entscheidet dann letztverbindlich über die Gewährung des Zugangs und stellt bei positivem Ausgang den Kontakt zur Plattform her.

Möglich, aber wohl unüblicher, wäre es auch, den Zugang unmittelbar bei dem Koordinator des Niederlassungsorts einzureichen. Dies spart den Weg über die deutschen (bisher unterbesetzten) Behörden, führt aber dazu, dass der Antrag nicht bereits vom nationalen Koordinator abgesegnet wurde – was den Prozess also an anderer Stelle verlängern könnte.

6. Delegierter Rechtsakt und offene Fragen

Zu den genauen Modalitäten des Zugangs nach Art. 40 Abs. 4 DSA gibt es noch viele Fragezeichen. Die Europäische Kommission ist nach Art. 40 Abs. 13 DSA beauftragt, die Details in einem delegierten Rechtsakt festzulegen. Erst mit dessen Einführung kann das neue Datenzugangsrecht tatsächlich genutzt werden. Nun hat die Kommission Ende Oktober 2024 einen Entwurf vorgestellt und um öffentliche Konsultation und Feedback gebeten.[9] Über 109 Rückmeldungen erreichten die Kommission. Bis Mitte 2025 sollen diese eingearbeitet werden und der finale Rechtsakt in Kraft treten. Während der Entwurf überwiegend positiv bewertet wird, bleiben doch einige Fragen offen.

Forschende des *DSA40 Data Access Collaboratory*[10] fordern eine Möglichkeit, den Antrag auf Datenzugang im Laufe des Forschungsprozesses anpassen zu können.[11] Plattformen haben dieses Recht nach Art. 40 Abs. 5 DSA, die Forschenden hingegen nicht. Dies werde den Anforderungen an flexible und agile Forschung, die es gerade in solchen Feldern braucht, nicht gerecht.

---

7 Selinger/Klinger/Ohme, Tech Policy Press, https://www.techpolicy.press/non-public-data-access-for-researchers-challenges-in-the-draft-delegated-act-of-the-digital-services-act/.

8 Hier findet sich die Anlaufstelle: https://www.dsc.bund.de/DSC/DE/_Home/start.html?r=1; hierzu von Bernuth, Kurzbeitrag: The floor is yours, Bundesnetzagentur, DFN-Infobrief Recht 08/2024.

9 Der Prozess und Entwurf sind hier nachzuvollziehen: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13817-Delegated-Regulation-on-data-access-provided-for-in-the-Digital-Services-Act_en.

10 Ein Verbund der Forschenden, die den Datenzugang nutzen wollen: https://dsa40collaboratory.eu.

11 Feedback zum Entwurf eines delegierten Rechtsakts, S. 4, abrufbar unter: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13817-Delegated-Regulation-on-data-access-provided-for-in-the-Digital-Services-Act/F3498940_de.

Ein kritischer Aspekt ist auch die Datenqualität.[12] Es sind bisher keine Mechanismen vorgesehen, die Forschenden erlauben, etwa die Vollständigkeit oder Authentizität der erhaltenen Daten zu überprüfen. Gerade weil es sich nicht nur um öffentliche Daten handelt, ist etwa ein Abgleich über selbst gesammelte Daten nicht möglich.

Eine zentrale Errungenschaft des delegierten Rechtsakts ist das DSA Data Access Portal.[13] In diesem Portal sollen alle erfolgreichen Datenzugangsanträge überblicksartig gesammelt werden – mit Hinweisen auf das Forschungsziel. So können die Forschenden einsehen, woran schon gearbeitet wird und wo gegebenenfalls noch Lücken bestehen. Wie das zahlreiche Feedback auf den delegierten Rechtsakt zeigt, steht die Forschungsgemeinschaft bereits in den Startlöchern – Zeit, dass die Kommission die nötigen Grundlagen schafft.

III. Der Zugang zu öffentlichen Daten

Das zweite Datenzugangsrecht ist in der Wissenschaft bereits im Einsatz. Es findet sich in Art. 40 Abs. 12 DSA und enthält das Recht auf Zugang zu öffentlich verfügbaren Daten. Vom Umfang der Daten ist es daher deutlich begrenzter und ermöglicht im Wesentlichen das, was einige Plattformen schon in der Vergangenheit zuließen. So hatte etwa Twitter (heute X) vor Übernahme durch Elon Musk lange eine Schnittstelle (API), über die Forschende die öffentlich zugänglichen Daten sammeln konnten. Zuletzt war aber die Arbeit mit öffentlich verfügbaren Daten deutlich mühsamer geworden und mit Rechtsunsicherheit behaftet.

1. Wer berechtigt und wer verpflichtet ist

Auch Art. 40 Abs. 12 DSA verpflichtet die sehr großen Online-Plattformen und Suchmaschinen zur Gewährung des Datenzugangs. Auf der Seite der Berechtigten ist die Norm aber etwas großzügiger als Art. 40 Abs. 4 DSA. Nicht erforderlich ist, dass die Antragstellenden mit einer Forschungseinrichtung im oben beschriebenen Sinne verbunden sind. Neben Forschenden von Organisationen der Zivilgesellschaft erfasst dieses Zugangsrecht auch sonstige Forschende, die individuell arbeiten.[14]

2. Bedingungen

Auch Art. 40 Abs. 12 DSA verweist aber auf einige der oben ausgeführten Bedingungen. So muss auch für den Zugang gem. Abs. 12 nachgewiesen werden können, dass Unabhängigkeit von kommerziellen Interessen besteht, die Finanzierung transparent ist und Anforderungen an die Datensicherheit und Vertraulichkeit gewährleistet sind. Außerdem gilt auch hier: Zweck muss die wissenschaftliche Erforschung von systemischen Risiken im Sinne der Art. 34, 35 DSA sein.

Hier ist die Verfahrenslogik dieses Datenzugangsrechts etwas unklar. Einerseits ist ein Antrag bei der Online-Plattform oder Koordinationsstelle nicht explizit vorgeschrieben. Auch mit Blick auf die Normhistorie und die Erwägungsgründe geht die Literatur daher weitgehend davon aus, dass das Zugangsrecht faktisch eher ein Anspruch auf Nicht-Verhinderung des Zugangs darstellt.[15] Ein formalisiertes Antragsverfahren sieht die Norm daher nicht vor.

Andererseits können sich die Online-Plattformen auf den Standpunkt stellen, dass die in der Norm genannten Voraussetzungen erst individuell geprüft werden müssen. Faktisch müssen die Forschenden bislang also auch für den Erhalt dieses Zugangsrechts einen Antrag bei der Plattform stellen.

Damit im Zusammenhang steht die Frage, ob die Norm auch ein eigenständiges Scraping der öffentlichen Daten umfasst. Scraping meint das automatisierte Auslesen und Speichern der öffentlich verfügbaren Daten einer Website mittels Software.[16] Legt man

12 Selinger/Klinger/Ohme, Tech Policy Press, https://www.techpolicy.press/non-public-data-access-for-researchers-challenges-in-the-draft-delegated-act-of-the-digital-services-act/.

13 Vermulen, Tech Policy Press, https://www.techpolicy.press/reading-the-european-commissions-proposed-implementation-of-dsa-article-40-six-initial-observations-on-a-new-framework-for-research-data-access/.

14 Dies hat etwa Relevanz für Forschende wie Travis Brown, hierzu von Bernuth, Forschung? Unerwünscht., DFN-Infobrief Recht 02/2025.

15 Oster, in: Gersdorf/Paal (Hrsg.), BeckOK Informations- und Medienrecht, 46. Edition, Art. 40 DSA, Rn. 43; mit Verweis auf Erwägungsgrund 98 Kaesling, in: Hofmann/Raue (Hrsg.), Digital Services Act, Art. 40 DSA, Rn. 92.

16 Siehe hierzu BGH, Urteil vom 18.11.2024 – VI ZR 10/24; Dallmann/Busse, ZD 2019, 394, 396.

Art. 40 Abs. 12 DSA im Sinne der weit vorherrschenden Literatur aus, würde das Scraping unter die Norm fallen. Angesichts der Historie der Norm, die ursprünglich einen Anspruch auf Nicht-Verhinderung vorsah, scheint dies auch der gesetzgeberischen Intention zu entsprechen. Das allerdings würde nicht davon entbinden, dass Forschende die Anforderungen zur Datensicherheit etc. erfüllen müssen. Möglich ist also, dass vor dem Scraping ein Antrag bei der Online-Plattform zu stellen ist.

3. Gerichtsbeschluss: X muss Zugang gewähren

Diese Unklarheiten werden durch die Rechtsprechung und die behördliche Aufsicht über den DSA geklärt werden müssen. Dazu hatte ein erstes Gericht bereits die Gelegenheit: Die Organisation Democracy Reporting International hat ein Eilverfahren gegen X vor dem Landgericht Berlin eingeleitet, weil die Plattform ihr den Zugang zu öffentlich verfügbaren Daten (Art. 40 Abs. 12 DSA) verweigert. Mit Unterstützung der Gesellschaft für Freiheitsrechte soll dieser Grundsatzprozess die Kooperationspflicht der Plattformen gerichtlich feststellen. Mit erstem Erfolg: Das Landgericht Berlin entschied zunächst zugunsten der Nichtregierungsorganisation.[17] X wehrte sich jedoch gegen die Entscheidung und konnte glaubhaft machen, dass der Richter befangen war – nicht jedoch, weil er in der Sache einseitig entschieden hätte, sondern wegen seines persönlichen Werdegangs.[18] Der Fall muss daher neu bewertet werden. Ob es in diesem Fall noch dazu kommt, ist fraglich: Der konkrete Zweck des Forschungsvorhabens dürfte sich mit Ablauf der Bundestagswahl erledigt haben. Auch der Gerichtsprozess um Travis Brown, vorgestellt im DFN-Infobrief 02/2024, zeigte schon, dass Forschende sich auf Gegenwehr der Plattformen einstellen müssen.[19]

IV. Fazit

Die Datenzugangsrechte bergen großes Potenzial für die Wissenschaft. Hochschulen und Forschungseinrichtungen können dabei besonders einfach die Anforderungen an den Datenzugang nachweisen, sie sind in der Regel unabhängig von kommerziellen Interessen. Dies setzt aber voraus, dass Forschende mit der entsprechenden technischen Infrastruktur ausgestattet werden, um die Anforderungen an Datensicherheit glaubhaft machen zu können. Das Interesse aus der Forschungsgemeinschaft, mit den Plattformdaten zu arbeiten, ist jedenfalls da. Nun kommt es auch darauf an, dass die Plattformen sich kooperativ zeigen oder anderenfalls die Kommission sie durch Aufsichtsmaßnahmen hierzu verpflichtet.

17 LG Berlin, Beschl. v. 06.02.2025 – 41 O 140/25 eV; abrufbar unter https://freiheitsrechte.org/themen/freiheit-im-digitalen/x (zuletzt abgerufen am 27.02.2025.

18 Zum Hintergrund: https://rsw.beck.de/aktuell/daily/meldung/detail/kg-berlin-x-richter-befangenheit-ablehnung (zuletzt abgerufen am 27.02.2025).

19 Hierzu von Bernuth, Forschung? Unerwünscht., DFN-Infobrief Recht 02/2025.

Das kann sich doch niemand merken

Diskussion zu Personenbezug in Large Language Models

Von Johannes Müller, Münster

Fortschrittliche, auf Künstlicher Intelligenz basierende, große Sprachmodelle (Large Language Models – LLMs) sind imstande, in Reaktion auf die Eingaben (Prompts) ihrer Nutzer Texte auf hohem sprachlichem Niveau zu verfassen. Die von dem Sprachmodell generierten Texte können regelmäßig personenbezogene Daten enthalten. Daher stellt sich die Frage, ob das Sprachmodell selbst personenbezogene Daten enthält. Dies hätte enorme Auswirkungen auf die Betreiber von LLMs, die ein KI-System mit einem LLM in eigener Verantwortung verwenden. Sie müssten etwa die datenschutzrechtlichen Betroffenenrechte erfüllen. Die Frage, ob ein Sprachmodell selbst personenbezogene Daten enthält, ist selbst unter Aufsichtsbehörden umstritten.

I. Ausgangsfrage

Die Texte, die von Sprachmodellen in Abhängigkeit zu den Eingaben generiert werden, können auch personenbezogene Daten enthalten. Im alltäglichen Gebrauch handelt es sich bei den Ausgaben personenbezogener Daten in vielen Fällen um Informationen zu Personen, an denen ein öffentliches Interesse besteht. Diese Informationen sind regelmäßig frei verfügbar. Auf die Eingabe „Manuel Neuers aktueller Beruf ist“ sollte ein funktionierendes LLM mit einer hohen Wahrscheinlichkeit das Wort „Fußballspieler“ generieren. Aufgrund der allgemeinen Verfügbarkeit dieser Information ist die Ausgabe weitestgehend datenschutzrechtlich unproblematisch. Dennoch handelt es sich hierbei um ein personenbezogenes Datum, sodass grundsätzlich der Anwendungsbereich der Datenschutzgrundverordnung (DSGVO) eröffnet ist. Hier stellt sich die Frage, ob das Sprachmodell selbst personenbezogene Daten gespeichert hat, da es offenbar den korrekten Beruf und damit personenbezogene Daten von Manuel Neuer kennt. Die gleiche Frage stellt sich auch für Ausgaben, die personenbezogene Informationen enthalten, die sich gegebenenfalls nicht auf Personen des öffentlichen Lebens beziehen. Sofern man zu dem Ergebnis kommt, dass das Sprachmodell selbst die personenbezogenen Daten gespeichert hat, könnte diese Datenverarbeitung bei sensiblen Informationen auch rechtswidrig sein.

II. „Speicherung“ von Wissen in LLMs

Für ein gutes Verständnis der datenschutzrechtlichen Diskussion um die Frage, ob LLMs selbst personenbezogene Daten speichern, ist es notwendig darzulegen, wie LLMs imstande sind, Texte zu generieren.

Das erforderliche „Wissen“ eines Sprachmodells, das ihm erlaubt, auf die Prompts eines Nutzers angemessen zu reagieren und die gewünschten Texte verfassen zu können, ist bei LLMs nicht statisch, etwa in Form einer Datenbank gespeichert. Stattdessen generiert das Sprachmodell Texte, indem es vor dem Verfassen jedes einzelnen Wortes die Wahrscheinlichkeit für das nächste Wort, beziehungsweise tatsächlich den nächsten Token (Tokens sind Sprachfragmente aus mehreren Buchstaben, ein Wort besteht in der Regel aus mehreren Tokens) berechnet und einen der Tokens mit der höchsten Wahrscheinlichkeit auswählt. In die Wahrscheinlichkeitsberechnung fließt der Prompt des Nutzers und der bereits durch den LLM verfasste Text mit ein. Hierauf aufbauend wird dann berechnet, welche Wortfolgen (eigentlich Tokenfolgen) am wahrscheinlichsten sind. Maßgeblich für die Frage, wie sich die bestehenden Worte (in dem Prompt und dem bereits gebildeten Text) auf die Wahrscheinlichkeit für den nächsten Token auswirken, sind die Parameter des Sprachmodells. Sie bilden den Kern des Modells und bestimmen darüber, wie gut das Sprachmodell imstande ist, den eingegebenen Text zu verstehen und die gewünschte und inhaltlich richtige Ausgabe

zu formulieren. Die veraltete Version Chat-GPT 3 arbeitete etwa mit 175 Milliarden Parametern. In den Parametern steckt das „Wissen“ des Sprachmodells, welches Wort üblicherweise einer bestimmten Frage oder einem Satzteil folgt.

Diese Parameter erhalten ihren jeweils konkreten Wert durch das Training des Sprachmodells.[1] Im Rahmen des Trainings werden große Mengen an Textdaten in die Eingabe des Modells gegeben. Dann werden die Ausgaben des Sprachmodells (also die berechnete Wahrscheinlichkeit für die nächste Wortfolge) mit dem Wort verglichen, das in dem Trainingstext tatsächlich folgt. Anschließend werden durch einen aufwändigen Algorithmus die Parameter des Modells so angepasst, dass das Modell imstande ist, die Wortfolgen möglichst präzise vorherzusagen, sodass der gesamte Unterschied zwischen der vorhergesagten und der tatsächlichen Wortfolge in allen Trainingsdaten immer kleiner wird. Hierdurch kann das Sprachmodell einerseits abstrakte Muster zwischen Wortfolgen erkennen und so etwa grammatikalische Regeln oder auch abstrakte Denkweisen erlernen (Generalization). Zum anderen lernt das LLM jedoch auch konkrete Fakten (Memorization). Diese Fakten können sich auch auf personenbezogene Informationen beziehen. Durch das Training sind also etwa die Parameter des Modells so eingestellt, dass das Modell vorhersagen kann, dass dem Satzanfang „Manuel Neuers aktueller Beruf ist“ mit einer sehr hohen Wahrscheinlichkeit das Wort „Fußballspieler“ folgt.

Juristisch umstritten ist hierbei aktuell die Frage, ob damit das Sprachmodell selbst in seinen Parametern auch personenbezogene Daten gespeichert hat.[2]

III. Auswirkungen der datenschutzrechtlichen Einordnung

Nimmt man an, dass ein Sprachmodell durch seine Parameter personenbezogene Daten enthält, stellt dieses Speichern eine Datenverarbeitung dar, sodass der Anwendungsbereich der DSGVO eröffnet ist. Demnach erfordert bereits der Betrieb des Sprachmodells in eigener Verantwortung (etwa auf eigenen Servern) eigene Rechtsgrundlagen für das Speichern der jeweiligen personenbezogenen Daten, die im Modell enthalten sind. Die Rechtmäßigkeit der Datenverarbeitung wird sich vor allem danach richten, auf welche Personen sich die Informationen beziehen und woher die Informationen stammen, also mit welchen Daten die Modelle trainiert wurden.

Selbst wenn sich das Speichern der personenbezogenen Daten auf eine Rechtfertigungsgrundlage stützen lässt, hat die Eröffnung des Anwendungsbereichs der DSGVO dennoch unterschiedliche rechtliche Folgen. Betroffene Personen können etwa von ihrem Auskunftsrecht gemäß Art. 15 DSGVO Gebrauch machen und vom Betreiber des KI-Systems die Bestätigung verlangen, ob personenbezogene Daten im Modell verarbeitet werden. Sofern die Daten nicht korrekt sind, könnte die betroffene Person ihr Recht auf Berichtigung gemäß Art. 16 DSGVO geltend machen. Besonders relevant ist auch das Recht auf Löschung gemäß Art. 17 DSGVO. Ob und in welchem Umfang spezifische Informationen aus einem Sprachmodell entfernt werden können, ist derzeit noch unklar.[3]

IV. Die Auffassung des Landesdatenschutzbeauftragten Hamburg

Am 15. Juli 2024 hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ein Diskussionspapier zu LLMs und personenbezogenen Daten veröffentlicht.[4] Hierin vertritt der Landesdatenschutzbeauftragte die Auffassung, dass in LLMs keine personenbezogenen Daten enthalten seien und deshalb auch das Speichern eines LLMs keine Verarbeitung im Sinne von Art. 4 Nr. 2 DSGVO darstellen würde. Er begründet dies damit, dass die Sprachmodelle nicht einfach einen gespeicherten Text wiedergeben, sondern eigenständige Texte formulieren und sich damit grundlegend von herkömmlicher Datenspeicherung unterscheiden würden. Die Texte bestünden lediglich aus einzelnen Tokens, die selbst keinen individuellen Informationsgehalt besäßen. Auch in der Beziehung dieser Tokens zueinander, also der Frage, mit welcher Häufigkeit bestimmte Wortfragmente

1 Vgl. zur urheberrechtlichen Zulässigkeit des KI-Trainings Müller, Die Menge macht’s, DFN-Infobrief Recht 11/2024.

2 In der rechtswissenschaftlichen Literatur setzt sich Pesch/Böhme, MMR 2023, 917 (920) mit dieser Frage auseinander.

3 Hierzu auch Heidrich, MMR 2024, 919.

4 Das Diskussionspapier kann unter folgendem Link abgerufen werden https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf (alle Links des Beitrags zuletzt abgerufen am 22.01.2025).

einem Satz folgen, sieht der Landesdatenschutzbeauftragte kein personenbezogenes Datum. Ihnen könne alleine keine Einzelinformationen über natürliche Personen entnommen werden. Stattdessen bezögen sich diese auf allgemeine Muster und Zusammenhänge.

Das Diskussionspapier geht auch auf Experimente ein, die zeigen sollen, dass durch gezielte Attacken LLMs teilweise ihre Trainingsdaten – auch solche mit Personenbezug – wiedergeben. Der Landesdatenschutzbeauftragte geht jedoch davon aus, dass diese nur zur wissenschaftlichen Forschung erfolgen und in der Praxis unverhältnismäßigen Aufwand erfordern würden, aufgrund dessen ein Personenbezug nicht angenommen werden dürfe.

Allerdings geht das Diskussionspapier nicht darauf ein, dass LLMs auch außerhalb von „Laborbedingungen" in ihrem täglichen Gebrauch personenbezogene Daten ausgeben, etwa auf die Frage, welchen Beruf Manuel Neuer ausübt. Auch dieses Wissen spiegelt die Trainingsdaten des Sprachmodells wider.

V. Die Auffassung des EDSA

Auch der Europäische Datenschutzausschuss (EDSA) hat sich mit personenbezogenen Daten innerhalb von Sprachmodellen auseinandergesetzt. Am 17. Dezember 2024 hat er eine Stellungnahme zu unterschiedlichen Datenschutzaspekten bei Datenverarbeitungen im Kontext von KI Modellen veröffentlicht.[5]

Hierbei teilt der EDSA nicht die grundsätzliche Ablehnung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit gegenüber der Ansicht, dass LLMs personenbezogene Daten speichern könnten. Stattdessen geht er davon aus, dass ein KI-Modell nicht anonym sei, also personenbezogene Daten enthält, sofern dem Modell mit verhältnismäßigem Aufwand personenbezogene Daten entnommen werden könnten.

Dem stehe nicht entgegen, dass die Informationen im Modell in Parametern vorkommen, die sich von den ursprünglichen Trainingsdaten in ihrer Darstellung unterscheiden. Sofern in der Ausgabe trotzdem personenbezogene Daten erzeugt würden, seien diese auch im Sprachmodell enthalten. Damit liegt ein wesentlicher Unterschied zu der Auffassung des Hamburger Beauftragten für Datenschutz und Informationsfreiheit in der Annahme, dass auch das Vorkommen der Informationen in Parametern nicht der Annahme von personenbezogenen Daten entgegenstehe.

Für die Frage, ob dem Modell unter verhältnismäßigen Aufwand personenbezogene Daten entnommen werden können, solle unter anderem berücksichtigt werden, mit welchen Kosten und Zeitaufwand eine Identifizierung möglich sei und welche Technologien hierfür tatsächlich verfügbar seien.

VI. Auswirkungen auf wissenschaftliche Einrichtungen

Auch für wissenschaftliche Einrichtungen ist die Frage von hoher Relevanz, ob LLMs selbst personenbezogene Daten enthalten.[6] Sofern Forschungseinrichtungen ein Sprachmodell – etwa ein Open-Source-Modell – auf ihren eigenen Servern betreiben, wären die Einrichtungen bei der Eröffnung des Anwendungsbereichs der DSGVO auch Verantwortliche für die Speicherung der personenbezogenen Daten. Damit müssten sie grundsätzlich sicherstellen, dass die Speicherung rechtmäßig ist. Zudem müssten sie evaluieren, ob und in welchem Umfang sie imstande wären, die Betroffenenrechte aus der DSGVO zu erfüllen.

---

5 Die „Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models" kann in englischer Sprache unter folgendem Link abgerufen werden https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf.

6 Vgl. auch zum Einsatz von KI in der Wissenschaft Schöbel, Der AI Act und die Wissenschaft, DFN-Infobrief Recht 02/2025.

Nur eine Schürfwunde?

BGH trifft erste Leitentscheidung zu den Facebook-Scraping-Verfahren

Von Ole-Christian Tech, Münster

Der Bundesgerichtshof (BGH) hat erstmals vom neuen Instrument des Leitentscheidungsverfahrens Gebrauch gemacht und sich der Facebook-Scraping-Verfahren angenommen. Dabei hat der BGH jedoch nicht nur Rechtssicherheit im Angesicht einer aktuellen Klagewelle geschaffen, sondern auch kontrovers diskutierte Fragen zur Ersatzfähigkeit immaterieller Schäden beantwortet. Diese Antworten werden die Praxis noch lange beschäftigen.

I. Die Facebook-Scraping-Verfahren[1]

In den Facebook-Scraping-Verfahren geht es um den Missbrauch der Telefonnummern-Suchfunktion auf Facebook, durch den die Daten von etwa 533 Millionen Nutzern unerlaubt von Dritten gesammelt und im Darknet verbreitet wurden. Da die Täter die Suchfunktion ausnutzten, die von Facebook in der Standardvoreinstellung eine Sichtbarkeit „für alle" vorsieht, um über millionenfach generierte Telefonnummern die Facebook-Profile der Nutzer ausfindig zu machen und dadurch öffentliche Informationen der Nutzer zu „schürfen", nennt man dieses Vorgehen auch „Scraping".[2]

Der Kläger im Ausgangsverfahren fühlte sich dadurch verletzt und forderte Schadenersatz nach Art. 82 Datenschutz-Grundverordnung (DSGVO) für den immateriellen Schaden, den ihm der Vorfall durch Ärger und Kontrollverlust über seine personenbezogenen Daten (Nutzer-ID, Vor- und Nachname, Arbeitsstätte und Geschlecht) verursacht hat. Darüber hinaus beantragte er im Wege der Feststellungsklage nach § 256 Abs. 1 Zivilprozessordnung (ZPO) die Feststellung, dass Facebook verpflichtet ist, ihm alle künftigen materiellen und immateriellen Schäden zu ersetzen und Maßnahmen zu ergreifen, um derartige Vorfälle zu verhindern.

Das Landgericht Bonn (LG) gab dem Kläger teilweise recht und sprach ihm 250 Euro Schadenersatz zu. In der Berufung vor dem Oberlandesgericht Köln (OLG) unterlag der Kläger jedoch. Das OLG argumentierte, dass der bloße Kontrollverlust nicht ausreiche, um einen immateriellen Schaden im Sinne der DSGVO zu begründen, und der Kläger nicht hinreichend dargelegt habe, dass er darüber hinaus psychische Beeinträchtigungen erlitten habe.

Schätzungen gehen davon aus, dass allein in Deutschland noch ca. 6.000 vergleichbare Klagen bei den Zivilgerichten anhängig sind.[3]

Mit Beschluss vom 31. Oktober hat der BGH das Verfahren dann schließlich zum Leitentscheidungsverfahren gemäß § 552b ZPO n.F. bestimmt.

II. Das Leitentscheidungsverfahren

Der am 24. Oktober 2024 neu eingefügte § 552b ZPO führt erstmals ein sog. Leitentscheidungsverfahren beim BGH ein. Dabei handelt es sich um ein zivilprozessuales Instrument zur Bewältigung von Massenverfahren. Hintergrund sind die bundesweit gehäuft auftretenden „Klagewellen", bei denen häufig eine Vielzahl von Zahlungsklagen gegen Unternehmen anhängig gemacht werden und die Instanzgerichte vor Herausforderungen

1 Siehe auch die Pressemitteilung des BGH vom 18.11.2024 Nr. 218/2024.

2 Zu einem solchen Verfahren vor dem OLG Hamm vom 15. August 2023, Az. 7 U 19/23 siehe bereits Tech, Was kratzt mich das? In: DFN-Infobrief Recht 10/2023.

3 So etwa https://www.haufe.de/recht/weitere-rechtsgebiete/wirtschaftsrecht/daten-scraping-bgh-urteil-zu-facebook_210_637702.html (alle Links dieses Beitrags zuletzt abgerufen am 17.02.2025); siehe auch Mantz, GRUR 2024, 1878 (1878).

stellen.[4] Eine abschließende Klärung durch den Bundesgerichtshof bleibt jedoch in vielen Fällen aus, da die Beklagten aus prozesstaktischen Gründen, d.h. zur Vermeidung einer negativen höchstrichterlichen Entscheidung, durch Vergleiche kurz vor der mündlichen Revisionsverhandlung vor dem Bundesgerichtshof, die sog. „Flucht aus der Revision“ antreten.[5]

Um diese Praxis zu beenden und die Zivilgerichte zu entlasten, ermöglicht § 552b ZPO nunmehr in Fällen, die Rechtsfragen für eine Vielzahl gleichgelagerter Verfahren betreffen, eine Leitentscheidung über diese Rechtsfragen durch Beschluss, vgl. § 565 Abs. 1 ZPO.[6]

III. Die zugrundeliegende Rechtsfrage

Neben zivilprozessualen Fragen, die vor allem die Bestimmtheit der vom Kläger gestellten Anträge und die Anforderungen an ein Feststellungsinteresse i.S.d. § 256 Abs. 1 ZPO betreffen, sieht der BGH folgende datenschutzrechtlichen Fragen aufgeworfen:[7]

a) Liegt in der Implementierung der sog. Kontakt-Import-Funktion in Verbindung mit der Standardvoreinstellung „alle“ ein Verstoß der Beklagten gegen die Datenschutz-Grundverordnung im Sinne des Art. 82 Abs. 1 DSGVO?

b) Ist der bloße Verlust der Kontrolle über die gescrapten und nunmehr mit der Mobiltelefonnummer des Betroffenen verknüpften Daten geeignet, einen immateriellen Schaden im Sinne des Art. 82 Abs. 1 DSGVO zu begründen? Falls ja, wie wäre der Ersatz für einen solchen Schaden zu bemessen?

c) Welche Anforderungen sind an die Substantiierung einer Schadenersatzklage nach Art. 82 Abs. 1 DSGVO zu stellen?

IV. Antworten des BGH

Zunächst stellt der BGH fest, dass die Implementierung der sog. Kontakt-Import-Funktion in Verbindung mit der Standardvoreinstellung „alle“ gegen den Grundsatz des Datenschutzes durch datenschutzfreundliche Voreinstellungen (Privacy by Default) gem. Art. 25 Abs. 2 S. 1 und 3 DSGVO verstößt.[8]

Der Fall der extensiven Voreinstellungen von sozialen Netzwerken ist ein Beispiel für eine Verletzung des Privacy by Default-Prinzips par excellence, da a priori vorgegebene Standardvoreinstellungen von den Betroffenen erfahrungsgemäß nur selten angepasst werden und damit systematisch zu einer extensiven Verarbeitung personenbezogener Daten führen.[9]

Aus selbigem Grund sieht der BGH hierin auch einen Verstoß gegen den allgemeinen Verarbeitungsgrundsatz der Datenminimierung.[10]

Der BGH lässt jedoch offen, ob dieser Verstoß ggf. im konkreten Fall durch eine Einwilligung des Klägers in die Verwendbarkeit seiner Telefonnummer im Rahmen der Suchbarkeitsfunktion gerechtfertigt sein könnte und überlässt diese Prüfung dem Berufungsgericht.[11]

Daneben - vom BGH aber nicht weiter geprüft - liegt auch ein Verstoß gegen den in Art. 32 Abs. 1 DSGVO geregelten Grundsatz der Sicherheit der Verarbeitung zumindest nahe. Die Kontakt-Import-Funktion wurde von Facebook trotz massenhafter missbräuchlicher Anfragen erst sehr spät ausgewertet und es wurden kaum Gegenmaßnahmen ergriffen.[12]
Deutlich aufsehenerregender sind sodann die Ausführungen des BGH zur Frage des Kontrollverlustes als ersatzfähigen immateriellen Schaden und der Ersatzhöhe.

---

4 Bundesrat Drucksache 375/23, 18.08.2023.

5 Hierzu insgesamt Vollkommer, NJW 2024, 3257 (3257) Rn 1.

6 Siehe auch Toussaint, FD-ZVR 2024, 824428.

7 Bundesgerichtshof, Beschluss vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:311024BVIZR10.24.0) S. 6f.

8 Bundesgerichtshof, Urteil vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:181124UVIZR10.24.0) Rz. 86.

9 Baumgartner/Gausling, ZD 2017, 308, (313); Bundesgerichtshof, Urteil vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:181124UVI ZR10.24.0) Rz. 89.

10 Bundesgerichtshof, Urteil vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:181124UVIZR10.24.0) Rz. 88.

11 Bundesgerichtshof, Urteil vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:181124UVIZR10.24.0) Rz. 91.

12 Mantz, GRUR 2024, 1878 (1879); siehe hierzu auch bereits Tech, Was kratzt mich das? In: DFN-Infobrief Recht 10/2023.

Gerade die deutschen Zivilgerichte haben sich in der Vergangenheit immer wieder schwergetan, den Betroffenen einen immateriellen Schaden zu ersetzen, und selbst im Falle der Ersatzfähigkeit, zuletzt überwiegend geringe Beträge zugesprochen. [13]

Der BGH richtet seine Rechtsprechung nun an den jüngsten Entscheidungen des Europäischen Gerichtshofs (EuGH) aus und versteht diesen so, dass durch „bloßen Verlust der Kontrolle" über die personenbezogenen Daten bereits ein ersatzfähiger Schaden entsteht.[14] Kriterien für die Bemessung der Höhe des Geldbetrags sind dann die etwaige Sensibilität der betroffenen Daten (insb. Art. 9 Daten), die typischerweise zweckgemäße Verwendung der Daten, die Dauer des Kontrollverlusts und die Möglichkeit der Wiedererlangung der Kontrolle.[15] Als weiteren Anhaltspunkt erkennt der BGH auch den hypothetischen Aufwand für die Wiedererlangung der Kontrolle, z. B. durch Änderung der Daten (im konkreten Fall ein Rufnummernwechsel) an.[16]
Übersetzt in eine konkrete Schadenshöhe äußert der BGH nun: „Äußerst zweifelhaft erscheint daher, ob hier eine Festsetzung in gegebenenfalls nur einstelliger Höhemit dem Effektivitätsgrundsatz zu vereinbaren wäre (…). Dagegen hätte der Senat von Rechts wegen keine Bedenken, den notwendigen Ausgleich für den eingetretenen Kontrollverlust als solchen in einem Fall wie dem Streitgegenständlichen in einer Größenordnung von 100 Euro zu bemessen."[17]
Gerade diese Ausführungen haben in der Praxis gemischte Reaktionen hervorgerufen. Ein bloßer Kontrollverlust soll demnach einen Schadenersatz in Höhe von 100 Euro rechtfertigen. Ein aktuelles Urteil des Europäischen Gerichts (EuG) vom 8. Januar 2025, Rs. T-354/22, sprach einem Kläger zuletzt sogar einen Betrag von 400 Euro für die Übermittlung einer dynamischen IP-Adresse in die USA zu.[18]

Schließlich beantwortet der BGH die in der Praxis immer wieder auftauchende Frage, wie der Kläger seinen immateriellen Schaden substantiieren, das heißt darlegen muss.

Das OLG hatte im Berufungsverfahren noch geurteilt, der Kläger habe den immateriellen Schaden in Form des Kontrollverlusts nicht ausreichend substantiiert dargelegt, da eine Telefonnummer kein per se sensibles Datum sei, sondern vielmehr gerade dem Zweck der Kontaktaufnahme mit anderen Personen diene.[19] Der Kläger müsse somit zunächst substantiiert darlegen, dass er zuvor Kontrolle über dieses Datum hatte und ihm dann durch diesen Kontrollverlust tiefergehende immaterielle Schäden entstanden sind. Die bloße Behauptung von Angst, Sorge und Unwohlsein genüge nicht, vielmehr müssten konkrete objektive Beweisanzeichen für das Vorliegen dieser Emotionen vorliegen, wobei selbst Spam-SMS und –Anrufe nicht genügen, solange diese lediglich aus Textbausteinen bestehen.[20]

Mit diesen sehr hohen Anforderungen habe das OLG die Darlegungsanforderungen überspannt und dem Kläger unzulässig hohe Hürden auferlegt.[21]

Der BGH hält es demgegenüber für ausreichend, wenn der Kläger angibt, seine Daten bisher bewusst und ausgewählten Personen zugänglich gemacht zu haben. Hierdurch kann die Kontrolle über die „eigenen" Daten bereits hinreichend substantiiert werden. Außerdem stellte der BGH klar, dass die Sensibilität eines Datums keine Auswirkungen auf die Substantiierungsanforderungen, sondern allenfalls auf die Höhe des Schadens hat.[22] Zudem erkennt der BGH Spam-SMS und –Anrufe, die ein erhöhtes Unsicherheitsempfinden in der elektronischen Kommunikation auslösen, als hinreichende Substantiierung an.[23]

---

13 Hierzu bereits Tech, Wie gewonnen, so zerronnen in: DFN-Infobrief Recht 04/2024.

14 Bundesgerichtshof, Urteil vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:181124UVIZR10.24.0) Rz. 84.

15 Bundesgerichtshof, Urteil vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:181124UVIZR10.24.0) Rz. 99.

16 Bundesgerichtshof, Urteil vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:181124UVIZR10.24.0) Rz. 99.

17 Bundesgerichtshof, Urteil vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:181124UVIZR10.24.0) Rz. 100.

18 EuG, Urteil vom 08.01.2025, Rs. T-354/22 (ECLI:EU:T:2025:4) Rz. 199.

19 Bundesgerichtshof, Urteil vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:181124UVIZR10.24.0) Rz. 11.

20 Bundesgerichtshof, Urteil vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:181124UVIZR10.24.0) Rz. 11.

21 Bundesgerichtshof, Urteil vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:181124UVIZR10.24.0) Rz. 41.

22 Bundesgerichtshof, Urteil vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:181124UVIZR10.24.0) Rz. 42.

23 Bundesgerichtshof, Urteil vom 31. Oktober 2024, Az. VI ZR 10/24 (ECLI:DE:BGH:2024:181124UVIZR10.24.0) Rz. 40.

V. Relevanz für wissenschaftliche Einrichtungen und Hochschulen

Mit seiner Entscheidung hat der BGH die Hürden für einen immateriellen Schadenersatz nach Art. 82 Abs. 1 DSGVO deutlich gesenkt. Diese Tendenz zeigt sich - noch verstärkt - auch auf europäischer Ebene mit dem jüngsten Urteil des EuG. Auch vor diesem Hintergrund bleibt die Entscheidung des OLG nach der Zurückweisung durch den BGH mit Spannung abzuwarten. In der näheren Zukunft wird sich zeigen, ob die neue Linie der Rechtsprechung tatsächlich zu einem höheren Schutzniveau für Betroffene und mehr Sicherheit im digitalen Umfeld führt oder lediglich als Aufruf zu einem „Art. 82 DSGVO—Glücksrittertum“ verstanden wird.

In jedem Fall zeigt das Urteil einmal mehr, wie wichtig technische und organisatorische Maßnahmen bei der Verarbeitung personenbezogener Daten sind. Gerade Hochschulen und öffentliche Einrichtungen, die als häufig öffentlich-rechtliche Einrichtungen zwar von Bußgeldern nach Art. 83 DSGVO, nicht aber von Schadenersatzansprüchen nach Art. 82 DSGVO befreit sind, sollten die Entwicklungen im datenschutzrechtlichen Schadenersatzrecht als ernstzunehmendes Haftungsrisiko und damit als Compliance-Aufgabe begreifen.

DFN Infobrief-Recht-Aktuell

• KI-Recht: EU-Kommission veröffentlichte am 4. Februar 2025 Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz (KI)

Mit den Leitlinien soll eine wirksame und einheitliche Anwendung des KI-Gesetzes in der gesamten Europäischen Union sichergestellt werden. Sie befassen sich mit Praktiken schädlicher Manipulation, Social Scoring und biometrischer Echtzeitidentifizierung. Die Auslegung soll dem Europäischen Gerichtshof vorbehalten bleiben. Die Leitlinien sollen jedoch den Interessenträgern helfen, die Anforderungen des KI-Gesetzes zu verstehen und einzuhalten.

Hier erhalten Sie den Link zu den Leitlinien:
https://ec.europa.eu/newsroom/dae/redirection/document/112366 (zuletzt abgerufen am 25.02.2025).

• Plattformregulierung: EU-Kommission leitet ein förmliches Verfahren gegen TikTok wegen eines mutmaßlichen Verstoßes gegen den Digital Services Act (DSA) ein

Die EU-Kommission hat am 17. Dezember 2024 ein förmliches Verfahren gegen TikTok eingeleitet, da die Online-Plattform mögliche Verstöße gegen die Pflicht sehr großer Online-Plattformen nach dem DSA nicht erfüllt hat. Sehr große Online-Plattformen sind nach Art. 35 DSA zu Risikominderungsmaßnahmen verpflichtet. Bei Feststellung systemischer Risiken sind diese Maßnahmen zu ergreifen, um die demokratische Resilienz der EU und ihrer Mitgliedstaaten zu stärken. Die Verfahrenseinleitung steht im Zusammenhang mit den rumänischen Präsidentschaftswahlen am 24. November 2024.

Hier erhalten Sie den Link zur Pressemitteilung:
https://germany.representation.ec.europa.eu/news/eu-kommission-leitet-formliches-verfahren-gegen-tiktok-wegen-risiken-bei-wahlen-ein-2024-12-17_de (zuletzt abgerufen am 25.02.2025).

• Arbeitsrecht: Digitales Zugangsrecht einer Gewerkschaft zum Betrieb

Das Bundesarbeitsgericht hat am 28. Januar 2025 – 1 AZR 33/24 - entschieden, dass Art. 9 Abs. 3 Grundgesetz (GG) einer Gewerkschaft zwar grundsätzlich die Befugnis gewähre, betriebliche E-Mail-Adressen der Arbeitnehmer zu Werbezwecken und für deren Information zu nutzen. Jedoch müssten auch die damit einhergehenden Grundrechte des Arbeitgebers aus Art. 14 und Art. 12 Abs. 1 GG sowie die Grundrechte der Arbeitnehmer aus Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG bzw. Art. 8 der Charta der Grundrechte der Europäischen Union im Wege der praktischen Konkordanz berücksichtigt werden. Es bestehe keine Verpflichtung eines Arbeitgebers, der für ihn zuständigen Gewerkschaft die dienstlichen E-Mail-Adressen seiner Arbeitnehmer mit dem Ziel der Mitgliederwerbung mitzuteilen.

Hier erhalten Sie den Link zur Pressemitteilung:
https://www.bundesarbeitsgericht.de/presse/digitales-zugangsrecht-einer-gewerkschaft-zum-betrieb/ (zuletzt abgerufen am 25.02.2025).

Kurzbeitrag: Das Ende der Cookie-Banner?

Die neue Einwilligungsverwaltungsverordnung soll die Flut von Cookie-Bannern reduzieren

von Philipp Schöbel, Berlin

Kurz vor dem Ende des Jahres 2024 wurde die vom Bundesministerium für Digitales und Verkehr vorgelegte Einwilligungsverwaltungsverordnung (EinwV)[1] vom Bundesrat gebilligt.[2] Sie soll ein alternatives Einwilligungsverfahren zu den prominenten Cookie-Bannern ermöglichen.

I. Ziel der Verordnung

Viele Nutzende fühlen sich durch die Cookie-Banner im Internet gestört. Mit der EinwV sollen diese reduziert werden. Mithilfe von sogenannten anerkannten Diensten soll es möglich werden, eine Einwilligung dauerhaft zu hinterlegen. So soll nicht jedes Mal ein Cookie-Banner beim Aufrufen einer Website erscheinen. Die Rechtsgrundlage für den Erlass der Verordnung ist § 26 Abs. 2 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG).[3]

II. Anerkannte Dienste

Bisher gibt es noch keine anerkannten Dienste. Die Verordnung soll das Bereitstellen dieser Dienste ermöglichen, aber nicht vorschreiben.[4] Ein Dienst zur Einwilligungsverwaltung ist eine informationstechnische Anwendung oder ein digitaler Dienst, die oder der es Endnutzer:innen ermöglicht, die Einstellungen der Endnutzer:innen zu verwalten. Die Verwaltung umfasst das Speichern, Übermitteln und Widerrufen der Einstellungen der Endnutzer:innen.[5] Der anerkannte Dienst zur Einwilligungsverwaltung soll bei der erstmaligen Inanspruchnahme eines digitalen Dienstes durch Endnutzer:innen die hierzu getroffenen Einstellungen speichern.[6] Bei jeder weiteren Nutzung des digitalen Dienstes übermittelt der anerkannte Dienst dann dem jeweiligen Anbieter die Einstellungen der Endnutzer:innen.[7]

Der Dienst darf die Einwilligung nur verwalten, wenn die Endnutzer:innen vor der Einwilligung durch den digitalen Dienst umfassend informiert wurden. So muss der/die Endnutzer:in etwa über die konkreten gespeicherten Informationen, die Zwecke der Speicherung oder die Widerruflichkeit der Einwilligung in Kenntnis gesetzt werden.[8]

Die Verordnung regelt zudem die Anforderungen an ein nutzerfreundliches Verfahren. So soll etwa die Benutzeroberfläche des Dienstes zur Einwilligungsverwaltung so transparent und

---

1 Verordnung über Dienste zur Einwilligungsverwaltung nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (Einwilligungsverwaltungsverordnung – EinwV).

2 BMDV, Pressemitteilung 20.12.2024, abrufbar unter: https://bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2024/073-wissing-wir-wollen-die-cookie-flut-reduzieren.html (alle Links dieses Beitrags zuletzt abgerufen am 31.01.2024).

3 Zum „neuen" TDDDG: Yang-Jacobi, Telemedien out, Digitale Dienste in!, DFN-Infobrief Recht 8 / 2024, S. 13.

4 Heise-online, Datenschutz: Bundestag stimmt Verordnung gegen Cookie-Banner-Flut zu, 18.10.2024, abrufbar unter: https://www.heise.de/news/Datenschutz-Bundestag-stimmt-Verordnung-gegen-Cookie-Banner-Flut-zu-9985448.html.

5 § 2 Abs. 1 Nr. 1 EinwV.

6 § 3 Abs. 1 S. 1 EinwV.

7 § 3 Abs. 1 S. 2 EinwV.

8 § 3 Abs. 2 EinwV.

verständlich gestaltet sein, dass der/die Endnutzer:in eine freie und informierte Entscheidung treffen kann.[9] Die Einstellungen der Endnutzer:in müssen von diesen jederzeit geändert und gegebenenfalls widerrufen werden können.[10] Der/die Endnutzer:in darf erst frühestens nach einem Jahr zur Überprüfung seiner/ihrer Einstellungen aufgefordert werden.[11] Dies gilt nur dann nicht, wenn der/die Endnutzer:in eine andere Einstellung vorgesehen hat.

Ebenfalls geregelt ist der Wechsel zu einem anderen anerkannten Dienst zur Einwilligungsverwaltung. Der/die Endnutzer:in kann den Dienst jederzeit wechseln und die getätigten Einstellungen auf den anderen anerkannten Dienst zur Einwilligungsverwaltung übertragen.[12] Der anerkannte Dienst zur Einwilligungsverwaltung ist verpflichtet, die Einstellungen in einem gängigen und maschinenlesbaren Format vorzuhalten.[13] Dem anderen anerkannten Dienst zur Einwilligungsverwaltung müssen diese Einstellungen kostenlos zum Abruf bereitgestellt werden, wenn der/die Nutzer:in dies verlangt.

Die Dienste müssen ein Sicherheitskonzept einhalten, dessen Anforderungen sich aus dem TDDDG ergeben.[14] Das Sicherheitskonzept muss eine Bewertung der Qualität und Zuverlässigkeit des Dienstes und der technischen Anwendungen ermöglichen. Zudem muss sich aus ihm ergeben, dass der Dienst sowohl technisch als auch organisatorisch die rechtlichen Anforderungen an den Datenschutz und die Datensicherheit erfüllt.

Die Einbindung von anerkannten Diensten zur Einwilligungsverwaltung durch Anbieter von digitalen Diensten erfolgt freiwillig.[15] Anbieter von digitalen Diensten, die einen anerkannten Dienst zur Einwilligungsverwaltung einbinden, sollen die Einstellungen der Endnutzer:innen berücksichtigen.[16] Zudem sollen sie nicht ohne sachlichen Grund darauf hinwirken, dass Endnutzer:innen bestimmte anerkannte Dienste zur Einwilligungsverwaltung anwenden oder ausschließen.[17]

III. Anerkennung von Diensten zur Einwilligungsverwaltung

Zuständig für die Anerkennung von Diensten zur Einwilligungsverwaltung ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI).[18] Die Anerkennung erfolgt elektronisch.[19] Das Formular für den Antrag auf Anerkennung eines Dienstes zur Einwilligungsverwaltung wurde von der BfDI bereits online gestellt.[20] Die BfDI informiert die zuständigen Aufsichtsbehörden der Länder elektronisch über die Anerkennung eines Dienstes zur Einwilligungsverwaltung.[21] Außerdem führt sie ein öffentliches Register der anerkannten Dienste zur Einwilligungsverwaltung[22] Dritte können der BfDI Hinweise auf und Beschwerden über mögliche Verstöße des anerkannten Dienstes zur Einwilligungsverwaltung elektronisch melden.[23] Die Anerkennung kann widerrufen werden.[24]

9 § 4 Abs. 1 Nr. 1 EinwV.

10 § 4 Abs. 1 Nr. 2 EinwV.

11 § 4 Abs. 2 EinwV.

12 § 5 Abs. 1 EinwV.

13 § 5 Abs. 2 EinwV.

14 § 26 Abs. 1 Nr. 4 TDDDG.

15 § 18 Abs. 1 EinwV.

16 § 19 Abs. 1 S. 1 EinwV.

17 § 20 EinwV.

18 § 8 EinwV.

19 § 11 Abs. 1 EinwV.

20 Das Formular ist abrufbar unter: https://formulare.bfdi.bund.de/lip/form/display.do?%24context=66C66B27D782B7CFD86A.

21 § 9 Abs. 1 EinwV.

22 § 13 EinwV.

23 § 15 Abs. 1 EinwV.

24 § 16 EinwV.

IV. Kritik anerkannte Dienste

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte schon während des Gesetzgebungsverfahrens Kritik an der Entwurfsversion der Einwilligung geäußert.[25] Teilweise wurden die vorgebrachten Kritikpunkte berücksichtigt. Erneute Kritik an der erlassenen Verordnung kommt nun unter anderem vom Landesbeauftragten für den Datenschutz Niedersachsen.[26] Dieser weist unter anderem darauf hin, dass wichtige Kritikpunkte der DSK in der erlassenen Verordnung nicht berücksichtigt wurden. Da die Einbindung von Einwilligungsmanagementdiensten durch Webseitenbetreiber freiwillig sei, bestehe die Gefahr, dass viele Anbieter weiterhin auf herkömmliche Einwilligungsbanner setzen. Bisher gäbe es keine Dienste, die die Anforderungen der Verordnung erfüllten, und es sei unklar, wer solche Dienste in Zukunft anbieten werde, insbesondere im Hinblick auf die strengen Zertifizierungsanforderungen. Die Einwilligungsverwaltungsdienste deckten nur Einwilligungen nach § 25 TDDDG ab, nicht jedoch Einwilligungen gemäß der Datenschutz-Grundverordnung (DSGVO). Die Dienste führten daher nicht zu einer Vereinfachung des Einwilligungsmanagements. Einwilligungen würden weiterhin ausschließlich über Einwilligungsbanner auf Webseiten erteilt werden. Die Einwilligungsdienste speicherten außerdem die im Einwilligungsbanner getroffenen Entscheidungen der Nutzenden und übermittelten den Einwilligungsstatus automatisch bei einem erneuten Aufruf der Webseite, sodass (erst) bei einem erneuten Seitenaufruf eine wahrnehmbare Wirkung eintrete. Daher sei davon auszugehen, dass sich die bisherige Praxis im Umgang mit Einwilligungen auf Webseiten kaum ändern wird.

25 Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Juli 2023, abrufbar unter: https://bmdv.bund.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-20/entwurf-einwilligungsverwaltungsverordnung-stellungnahme-9.pdf?__blob=publicationFile.

26 Der Landesbeauftragte für den Datenschutz Niedersachsen, Pressemitteilung, 27.12.2024, abrufbar unter: https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/verabschiedete-einwilligungsverwaltungsverordnung-verfehlt-ihr-eigentliches-ziel-238383.html.

Impressum

Herausgeber

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

Texte:

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