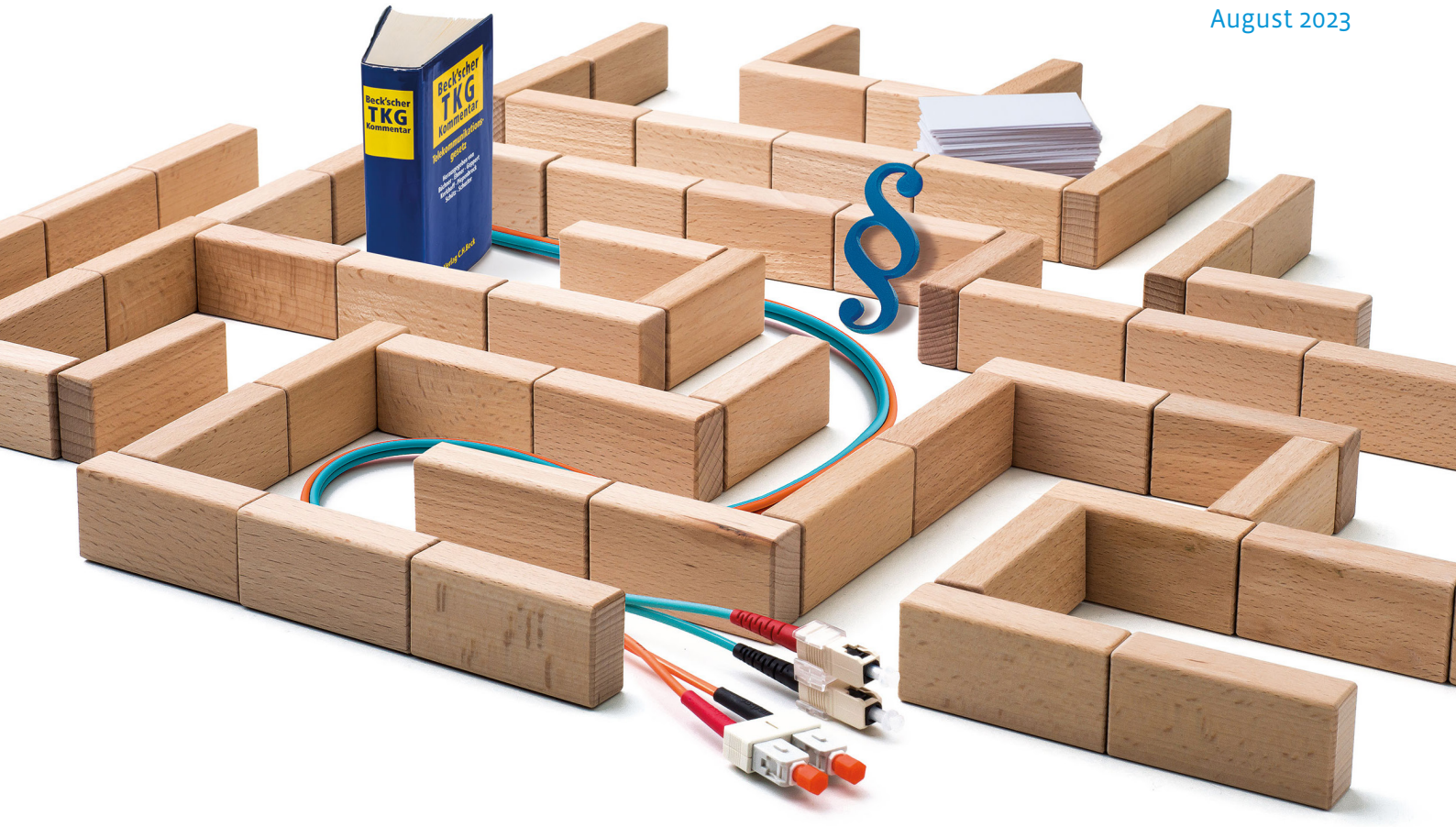
NEU: Podcast der
Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

DFN infobrief recht

8 / 2023
August 2023



Datenstaat oder Datensalat?

Ein Überblick über das neue Datenrecht in der Europäischen Union

Unforgettable – ein Beweis zum Vergessen

Der BGH entscheidet über die Auslistungspflichten von Google

Hier werden keine Daten gecloud

DSK stellt Positionspapier zur Nutzung von souveränen Clouds vor

Kurzbeitrag: Patient Patentrecht

Vorschlag der EU-Kommission für neue Patentvorschriften

Datenstaat oder Datensalat?

Ein Überblick über das neue Datenrecht in der Europäischen Union

von Ole-Christian Tech

Von Datenschutzgrundverordnung (DSGVO) über Digital Services Act (DSA), Digital Market Act (DMA) bis hin zu den sektorspezifischen Regulierungsansätzen wie den European Health Data Act (EHDS): Die EU Kommission hat in den letzten Jahren einen regelrechten Regulierungs-Tsunami für das relativ neue Gebiet des Datenrechts ausgelöst. Grund genug sich einen ersten Überblick im Regulierungsdschungel zu verschaffen.

I. Problemaufriss

Die 20er Jahre des laufenden Jahrhunderts sollen die digitale Dekade werden-so jedenfalls das erklärte Ziel der Europäischen Kommission. Um das ausgerufene Ziel zu erreichen, entzündet die Kommission ein regelrechtes Feuerwerk an Datenrechtsakten. Nach der DSGVO folgen nun die Free-Flow-of-Data-Verordnung (FFD), um nationale Datenlokalisationsgebote abzuschaffen, die Open-Data- und PSI-Richtlinie (PSI), um erstmals einen Rechtsrahmen für offene Daten zu schaffen, der Data Governance Act (DGA), welcher Bedingungen für die Weiterverwendung von Daten des öffentlichen Sektors und den Datenaltruismus festlegt, der Digital Markets Act (DMA), der mit Ge- und Verboten für große Onlineplattformen die Marktmacht regulieren soll, der Digital Services Act gegen Desinformation und Hassrede im Netz und viele weitere mehr.

II. Der AI-Act[1] - erster seines Namens[2]

Der Entwurf der Verordnung über Künstliche Intelligenz der EU-Kommission ist der erste Regulierungsrahmen für KI Systeme weltweit und schafft einen EU-weit harmonisierten Rechtsrahmen für den Einsatz künstlicher Intelligenz (Artificial Intelligence). Dabei sollen die KI-Systeme sicher und grundrechtskonform operieren. Durch diese gemeinsamen Standards soll ein funktionierender Binnenmarkt ermöglicht werden.

Dabei adressiert der Entwurf der KI-Verordnung die Anbieter von KI-Systemen, die in der EU in Verkehr gebracht wurden, die Nutzer von KI-Systemen, die sich in der EU befinden, sowie Anbieter und Nutzer von KI-Systemen, die in einem Drittstaat niedergelassen sind, wenn das Ergebnis in der EU verwendet wird.
Der gewählte Regelungsansatz ist risikobasiert (sog. risk based approach) und gliedert sich in verschiedene Kategorien von KI.

1. Verbotene Praktiken (Art. 5)

Verbotene Praktiken ist der Einsatz solche Systeme, die aufgrund ihres Risikos nie eingesetzt werden dürfen. Beispielsweise sind davon solche Systeme umfasst, die durch Beeinflussung einer Person dieser schaden können oder zur Bewertung von Zuverlässigkeit durch Behörden dienen. Biometrische Echtzeit-Fernidentifizierungssysteme zur Strafrechtspflege in öffentlichen Räumen sind grundsätzlich verboten und nur unter engen Voraussetzungen ausnahmsweise zulässig.

2. Hochrisiko-KI-Systeme

Die Verwendung Hochrisiko-KI-Systeme ist hingegen unter Beachtung weiterer Anforderungen grundsätzlich möglich. Dies umfasst beispielsweise die biometrische Identifizierung und Kategorisierung natürlicher Personen, Verwaltung und Betrieb

1 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206 (zuletzt abgerufen 12.07.2023).

2 Vertiefend hierzu Rennert, One KIss is all it takes, DFN-Infobrief Recht 1/2023.

kritischer Infrastruktur oder die allgemeine und berufliche Bildung. Als Pflichten soll es insbesondere ein Risikomanagementsystem, Transparenzpflichten sowie Anforderungen an die Trainingsdaten geben. Dadurch soll verhindert werden, dass die KI eine „Black Box“ ist.

3. Transparenzpflichten für bestimmte KI-Systeme

Art. 52 des Entwurfs statuiert Transparenzpflichten für bestimmte KI-Systeme. Dies umfasst beispielsweise Deepfakes, Emotionserkennungssysteme oder Systeme zur biometrischen Kategorisierung. Dadurch soll das Ziel der Erkennbarkeit des Einsatzes von KI erreicht werden.
Dabei ist jedoch bereits im Entwurf angelegt, dass die Transparenzpflicht für Deepfakes dann nicht gilt, wenn sie gesetzlich für die Strafverfolgung genutzt werden darf oder zur Verwirklichung von Meinungs-, Kunst- oder Wissenschaftsfreiheit notwendig ist.

4. KI-Reallabore

Ferner sollen KI-Reallabore eingerichtet werden, die Innovation bewirken sollen (Art. 53, 54). Auch für Hochschulen und Forschungseinrichtungen ergeben sich beim Einsatz künstlicher Intelligenz, in der Bildung, etwa bei der Bewertung von Eignungen oder in der Forschung mit Big Data neue Rechtspflichten. Der Einsatz dieser Systeme könnte hier in Teilen unter die strengeren Vorschriften für Hochrisiko-KI-Systeme fallen.

III. Der Digital Services Act (DSA)[3] - der neue Sheriff

Das Gesetz über digitale Dienste ist seit dem 1. November 2022 in Kraft und soll nach selbsterklärter Zielsetzung einen europaweit einheitlichen Rechtsrahmen für Verbraucherschutz, Grundrechtsschutz, Haftung und Sicherheit auf digitale Plattformen bzw. für digitale Dienste und Produkte schaffen.

So sieht die Kommission den DSA etwa als Sheriff in Sergio Leones Westernklassiker „zwei glorreiche Halunken“[4], der nun Recht und Ordnung in den „wilden Westen“ des digitalen Binnenmarktes bringen soll.

Betroffen sind hiervon digitale Vermittlungsdienste, also Internetzugangsdienste, soziale Netzwerke, Online-Marktplätze und Suchmaschinen, für die nun klare Sorgfaltspflichten gelten sollen. Zudem kann jeder Nutzer illegale Inhalte melden und die Inhaltemoderation der Plattformbetreiber (z. B. bei vermeintlich unrechtmäßiger Sperrung von Inhalten) anfechten und an außergerichtlichen Streitschlichtungsmechanismen teilnehmen.

IV. Der Digital Market Act (DMA)[5] - Regulierung der Torwächter[6]

Der Digital Market Act (DMA) ist seit dem 16. November 2022 in Kraft und soll die Marktmacht systemrelevanter Plattformen regulieren. Diese sog. „Gatekeeper“ sind Betreiber zentraler Plattformdienste, die erhebliche Auswirkungen auf den Binnenmarkt haben, einen zentralen Plattformdienst betreiben, der gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern dient und hinsichtlich ihrer Tätigkeiten eine gefestigte und dauerhafte Position innehaben oder innehaben werden.

Etwas greifbarer werden diese Kriterien durch die gesetzliche Vermutung in Artikel 3 Abs. 2 DMA, wonach drei Kriterien erfüllt werden müssen:

1. Ein Größenkriterium: Gatekeeper müssen einen Jahresumsatz von mindestens 6,5 Mrd. EUR im europäischen Wirtschaftsraum erzielt haben oder der durchschnittliche Marktwert des Unternehmens muss im vergangenen Geschäftsjahr mindestens 65 Mrd. EUR betragen haben.

2. Ein Gateway-Kriterium: Zudem muss der Gatekeeper im vergangenen Geschäftsjahr mehr als 45 Millionen in der Union aufhältige, monatliche aktive Endnutzer und mehr als 10 000 in der Union niedergelassene jährlich aktive, gewerbliche Nutzer haben.

---

3 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0825 (zuletzt abgerufen am 12.07.2023).

4 https://twitter.com/ThierryBreton/status/1483786510214303744?s=20 (zuletzt abgerufen am 12.07.2023).

5 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0842 (zuletzt abgerufen am 12.07.2023).

6 Vertiefend hierzu Rennert, Brüssel reguliert das schon, DFN-Infobrief Recht 6/2022.

3. Ein Dauerkriterium: Das Gateway-Kriterium muss in den letzten drei Geschäftsjahren erfüllt worden sein.

Als Rechtsfolge unterliegen Gatekeeper dann zahlreichen, oftmals bereits aus dem Kartellrecht bekannten Pflichten. Diese finden sich in Art. 5 ff. DMA und umfassen exemplarisch etwa ein Verbot der Datenkombination, die Verpflichtung, Kommunikation an Endnutzer zu erlauben, Koppelungsverbote, ein Verbot der Datennutzung im Wettbewerb, die Verpflichtung, Installation von Apps zu erlauben (Side Loading) und viele mehr.

Die Sanktionsmechanismen sind bereits aus dem europäischen Kartellrecht bekannt, so drohen bei Verstößen Bußgelder i.H.v. bis zu 10% des weltweiten Konzernumsatzes, bei wiederholten Verstößen bis zu 20%.

Der DMA gilt ab dem 2. Mai 2023. Nach der Benennung durch die Kommission als Gatekeeper müssen sich diese mit Ablauf einer sechs Monatsfrist an die Verpflichtungen halten. Damit wird der DMA etwa ab März 2024 seine volle Wirkung entfalten.

V. Der Data Act- the Big Fundamental

Am 23.02.2022 hat die EU-Kommission einen Entwurf zum Data Act veröffentlicht. Dabei soll ein unionsweiter Rahmen geschaffen werden, der den Zugriff auf Daten regulieren soll. Somit soll eine Wertschöpfung aus Daten durch verschiedene Akteure ermöglicht werden. Es zielt damit auch darauf ab, dass erhobene Daten optimal genutzt werden.
Dabei gibt es verschiedene Vorgaben je nachdem, welches Verhältnis betroffen ist.

1. Datenweitergabe im Verhältnis B2B und B2C

Die Vorgaben hierfür sind durch das Design, vorvertragliche Informationspflichten, das Recht auf Zugang zu während der Nutzung erzeugten Daten und Vorgaben für Drittnutzer der Nutzerdaten. Dadurch soll den Nutzern ein selbstbestimmter Umgang mit den Daten ermöglicht werden.

2. Bereitstellung von Daten durch Dateninhaber

Auch für Dateninhaber gibt es teils Limitationen beziehungsweise Bestimmungen über die Bereitstellung ihrer Daten. So soll hier der FRAND-Einwand (fair, reasonable and non-disciminatory) für die Vergabe von Nutzungsrechten gelten sowie das Verbot der Exklusivitätsbereitstellungen. Dadurch soll mehr Wettbewerb auch in Branchen ermöglicht werden, die in ihrer Entwicklung auf geschützte Datenbestände angewiesen sind.
Daher zielt der Data Act vor allem auf Datenzugangsrechte ab. Daneben gibt es weitere Vorschriften, beispielsweise für den Datenzugang für die Strafverfolgung.

VI. Die Free-Flow-of-Data-Verordnung (FFD)[7] - die Daten sind frei

Regelungsziel der Free-Flow-of-Data-Verordnung (FFD) vom 14. November 2018 ist der freie Verkehr nicht-personenbezogener Daten innerhalb der EU, um so einen digitalen Binnenmarkt zu stärken.
Hintergrund ist, dass es in einigen Mitgliedstaaten sog. Datenlokalisierungsauflagen gibt, die eine Verarbeitung bestimmter Daten nur im Inland erlauben und einen Transfer –wie etwa bei der Nutzung eines Clouddienstes in einem anderen EU Mitgliedstaat- verbieten.
In Deutschland galt eine solche Regelung z. B. für bestimmte Sprachkommunikationsdaten in § 176 Telekommunikationsgesetz (TKG).
Um sicherzustellen, dass nationale Behörden dennoch Zugriff auf die in einem anderen Mitgliedstaat gespeicherten Daten haben, sieht die Verordnung Zugriffsrechte und einen Rechtsrahmen für die Zusammenarbeit zwischen den Behörden vor.

VII. Die Open-Data- und PSI-Richtlinie (OD-PSI-RL)[8] - offen und öffentlich[9]

Die Open-Data- und PSI-Richtlinie ist die Richtlinie über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Public Sector Information) und fördert die

7 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018R1807&from=FI (zuletzt abgerufen am 12.07.2023).

8 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L1024&from=DE (zuletzt abgerufen am 12.07.2023).

9 Vertiefend hierzu McGrath, Data Unchained, DFN-Infobrief Recht 1/2022.

Offenlegung und Nutzung von öffentlich zugänglichen Daten. Der Anwendungsbereich der Richtlinie umfasst öffentliche Stellen wie Behörden, Ministerien und Organisationen, die öffentliche Dienste erbringen und Informationen sammeln.

Ziel ist es, den Zugang zu öffentlichen Daten zu erleichtern und deren Wiederverwendung zu fördern, indem öffentliche Stellen dazu verpflichtet werden, bestimmte Arten von Daten, die sie im Rahmen ihrer Aufgaben sammeln und verwalten, der Öffentlichkeit zur Verfügung zu stellen. Dazu gehören etwa Informationen über Umwelt, Wetter, Verkehr, Gesundheit, Finanzen und andere Bereiche des öffentlichen Interesses.

Durch die Wiederverwendung offener Daten sollen ungenutzte Potentiale entfaltet werden, deren (Sekundär-)Nutzung dann dazu beiträgt wichtige Belange des Allgemeinwohls zu fördern, wie künstliche Intelligenz zu entwickeln und Arbeiten zur Bewältigung gesellschaftlicher Herausforderungen zu unterstützen. Insbesondere für Forschungseinrichtungen und öffentlich finanzierte Forschung postuliert die Richtlinie daher den Grundsatz „so offen wie möglich, so geschlossen wie nötig“ (as open as possible, as closed as necessary).

Die Richtlinie enthält Bestimmungen zur Bereitstellung von Daten in maschinenlesbaren Formaten, um die Weiterverwendung und Verarbeitung der Daten zu erleichtern. Hierbei sind die Daten zwar nach Art. 6 Abs. 1 OD-PSI-RL grundsätzlich kostenfrei zur Weiterverwendung zur Verfügung zu stellen, jedoch können durch notwendige Verarbeitungsschritte wie Anonymisierung oder Umformatierung entstandene Kosten die Erhebung eines Entgelts rechtfertigen. Außerdem sieht die Richtlinie auch Mechanismen vor, um sicherzustellen, dass die bereitgestellten Daten zu fairen Bedingungen genutzt werden können, wie etwa die Förderung der Verwendung von Standardlizenzen.

Die Open-Data- und PSI-Richtlinie zielt also darauf ab, Innovationspotenziale aus öffentlichen Daten zu erschließen und die Transparenz der Datenverarbeitung im öffentlichen Sektor zu erhöhen. Die Richtlinie trägt damit zur Schaffung eines offenen und transparenten digitalen Binnenmarkts bei und fördert die Zusammenarbeit zwischen den Mitgliedstaaten der Europäischen Union im Bereich der offenen Daten.

VIII. Der Data Governance Act (DGA)[10] - durch Austausch entsteht Gewinn

Der Data Governance Act (DGA) trat am 23. Juni 2022 in Kraft und soll die Grundlage eines gesamteuropäischen Datenaustauschs schaffen. Hierdurch sollen sektorübergreifend Effizienzgewinne erzielt werden, indem etwa Daten zwischen Unternehmen geteilt werden oder aus dem öffentlichen Sektor zur Weiterverwendung in der Wirtschaft und Forschung bereitgestellt werden.
Als weiteres Instrument sieht der DGA eine freiwillige Datenspende vor, diese Art des Datenaltruismus soll die Datenverfügbarkeit im Zusammenhang mit Belangen des Allgemeinwohls, also z. B. öffentliche Gesundheit. Umwelt oder Klimaschutz erhöhen.
Außerdem wird in Art. 26 DGA ein Europäischer Dateninnovationsrat eingerichtet, der sich aus Vertretern und Experten der Mitgliedstaaten zusammensetzt und die Europäische Kommission beratend bei der praktischen Umsetzung der Dateninfrastruktur unterstützt.

IX. Die sektorspezifischen Regulierungsansätze, insbesondere der European Health Data Act (EHDS)[11] - no one fits all

Um für bestimmte Sektoren granularer regulieren zu können, plant die EU Kommission in den nächsten Jahren zudem die Einrichtung von zwölf großen Datenräumen und veranschlagt hierfür ein Umsetzungsbudget von fast einer Milliarde Euro. In den Datenräumen sollen besonders wichtige Datenkategorien in einem einheitlichen Datenformat und Syntax interoperabel gemacht und zu festgelegten Zwecken geteilt werden.

Der erste dieser Datenräume soll der EHDS werden, ein europäischer Raum für Gesundheitsdaten. Die EHDS Verordnung sieht dabei zwei Mechanismen vor, die Primärnutzung von Gesundheitsdaten (MyHealth@EU) und die Sekundärnutzung (HealthData@EU). Während auf der Primärebene die Daten für den ursprünglichen Zweck (etwa die Behandlung im Krankenhaus) erfasst, in einem europaweit einheitlichen Format gespeichert und EU-weit abrufbar gemacht werden, schafft die Sekundärebene ein echtes Novum: Eine europaweit einheitliche Datenteilungsinfrastruktur, die es Forschern erlaubt

10 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0767 (zuletzt abgerufen am 12.07.2023).

11 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0197 (zuletzt abgerufen am 12.07.2023).

Datenzugangsansprüche bei Datenzugangsstellen zu stellen und ihnen -bei einer Genehmigung durch diese- eine Art Herausgabeanspruch gegen den Dateninhaber gibt.

Hierdurch sollen erhebliche Fortschritte in der datengetriebenen Gesundheitsforschung entstehen, etwa die Ermöglichung bestimmter Studien, wie Untersuchungen zu unentdeckten Nebenwirkungen und Wechselwirkungen, die erst mithilfe großer Datensätze offenbart werden. Dies betrifft insbesondere die Forschung an extrem seltenen Erkrankungen, für die es in den einzelnen Mitgliedstaaten jeweils für sich genommen nicht genug Datensätze gibt.

X. Die NIS-2 Richtlinie[12] - safety first

Die im Januar 2023 in Kraft getretene NIS 2-Richtlinie ist die Neuauflage der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union. Sie legt Mindeststandards für die Cyber Sicherheit sog. Betreiber kritischer Infrastrukturen fest und geht dabei deutlich über den Anwendungsbereich der vorherigen NIS Richtlinie hinaus, so müssen ab 2024 zahlreiche Unternehmen in 18 Sektoren und ab 50 Mitarbeitern und 10 Mio. EUR Umsatz die neuen Vorgaben umsetzen. Da es sich um eine Richtlinie handelt, die anders als eine Verordnung nicht unmittelbar die Unionsbürger bindet, sondern sich an die Mitgliedsstaaten richtet und von diesen in nationales Recht umzusetzen ist, ist auf nationaler Ebene in Deutschland das Umsetzungsgesetzes zur NIS2-Richtlinie abzuwarten.[13]

Die NIS 2-Richtlinie legt strenge Anforderungen an die Sicherheitsvorkehrungen fest, die die Betreiber kritischer Dienste und digitale Diensteanbieter erfüllen müssen. So verpflichtet die Richtlinie diese, etwa technische und organisatorische Maßnahmen wie Risikomanagement- und Sicherheitsmaßnahmen einzuführen, um Cyberangriffe zu erkennen, darauf zu reagieren und ihre Auswirkungen zu mitigieren. Darüber hinaus müssen auch geeignete Mechanismen zur Meldung von Sicherheitsvorfällen eingerichtet werden.

Zudem sieht die Richtlinie auch Bestimmungen zur engeren Zusammenarbeit und zum Informationsaustausch zwischen den Mitgliedstaaten vor, wie die Einrichtung von nationalen Behörden für Netzwerk- und Informationssicherheit sowie ein Kooperationsnetzwerk, um sicherheitsrelevante Informationen auszutauschen und koordinierte Maßnahmen zur Bekämpfung von Cyberbedrohungen zu ergreifen.

Die NIS 2-Richtlinie zielt damit vor allem darauf ab, die Resilienz und Sicherheit der digitalen Infrastruktur zu stärken, den Schutz kritischer Dienste und Systeme vor Cyberangriffen zu verbessern, das Vertrauen der Verbraucher und Unternehmen in digitale Dienste nachhaltig zu erhöhen und die effektive Zusammenarbeit zwischen den Mitgliedstaaten zu fördern, um eine wirksame Reaktion auf Cyberbedrohungen zu gewährleisten.[14]

Bildlich gesprochen ist die die NIS-2 Richtlinie also der Schlussstein im Kuppelbau des digitalen Binnenmarktes, der die umfangreiche Digitalstrategie trägt und zusammenhält.

XI. Fazit

Die ambitionierte Digitalstrategie der Europäischen Union zeigt welches innovative und ökonomische Potential man in einem digitalen Binnenmarkt der Zukunft sieht. Es stehen Zahlen im Raum wie 550 Milliarden Euro Umsatz in der Datenwirtschaft bis 2025 und milliardenschwere Infrastrukturprojekte, um diese zu realisieren.

Aus Sicht von Gesellschaft, Forschung und Digitalwirtschaft ist ein umfassender Regulierungsrahmen grundsätzlich zu begrüßen. Fraglich bleibt jedoch, ob dieser angesichts seiner schnellen Umsetzungsfrist und der großen Ambitionen ausgereift genug ist, einen international wettbewerbsfähigen europäischen Datenstaat zu schaffen, oder ob sich das europäische Datenrecht zu einem regelrechten Datensalat entwickelt- inklusive aller Rechtsunsicherheiten und Innovationshindernisse.

---

12 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555 (zuletzt abgerufen am 12.07.2023).

13 Der Referentenentwurf aus dem Bundesministeriums des Innern, für Bau und Heimat ist abrufbar unter https://intrapol.org/wp-content/uploads/2023/05/NIS2UmsuCG.pdf (zuletzt abgerufen am 12.07.2023).

14 Vertiefend hierzu John, CSIRT, ENISA, BSI, IKT, UNIBÖFI – NSI?, DFN-Infobrief Recht 4/2023.

Unforgettable – ein Beweis zum Vergessen

Der BGH entscheidet über die Auslistungspflichten von Google

von Nicolas John

Das sog. „Recht auf Vergessenwerden“ spielt vor den höchsten Gerichten in den vergangenen Jahren immer wieder eine Rolle. So kam es jetzt wieder zu einem neuen Urteil des Bundesgerichtshofs (BGH), welches die Voraussetzungen für die Auslistungspflichten für die Suchergebnisse von Google weiter konkretisiert. Dieser Entscheidung ging eine Vorlage an den Gerichtshof der Europäischen Union (EuGH) voraus. Nach dessen Urteil konnte nun der BGH final entscheiden. Und so viel sei vom Ergebnis des Urteils vorweggenommen: Die Klage hatte nach vier verschiedenen Gerichtsbarkeiten und über acht Jahren Prozesszeit letztendlich teilweise Erfolg.

I. Das Recht auf Vergessenwerden

Das Recht auf Vergessenwerden ist für treue Leser:innen des DFN-Infobriefs Recht kein unbekannter Begriff. So war dieses in der Vergangenheit schon öfter Thema diverser Beiträge im DFN-Infobrief Recht.[1] Dennoch sei an dieser Stelle in gebotener Kürze auf die groben Grundlagen einzugehen, bevor sich dem Urteil des BGH gewidmet wird.

Hintergrund des Rechts auf Vergessenwerden ist der Wunsch einer Person, dass bestimmte Informationen über sie im Internet nicht mehr verfügbar sind. Doch gegen die einzelnen Webseiten, Plattformen oder sonstigen Betreibenden vorzugehen, kann mitunter anspruchsvoll, teuer und oftmals aufgrund verschiedener Hindernisse, wie z. B. fehlende Informationen über den Webseitenbetreibenden nicht erfolgreich sein. Daher wenden sich die betroffenen Personen oft gegen die Suchmaschinenbetreibenden. Denn indem die Suchmaschinen die unliebsamen Informationen nicht mehr in ihren Suchergebnissen listen, ist die Auffindbarkeit der eigentlich zu löschenden Daten für die Allgemeinheit bedeutend erschwert und kommt auf diese Weise der eigentlichen Löschungsabsicht recht nahe.

Juristisch findet das Recht auf Vergessenwerden seinen Anker für natürliche Personen in der Datenschutz-Grundverordnung (DSGVO), genauer in Art. 17. Dieser gibt der betroffenen Person das Recht vom Verantwortlichen zu verlangen, dass die personenbezogenen Daten unverzüglich gelöscht werden müssen. Damit dieses Recht besteht, muss einer der Gründe aus Art. 17 DSGVO vorliegen. Dies ist insbesondere dann der Fall, wenn die personenbezogenen Daten für die Zwecke, für welche sie erhoben wurden, nicht mehr notwendig sind, die Einwilligung von der betroffenen Person widerrufen wird, Widerspruch gegen die Verarbeitung eingelegt wurde und keine berechtigten Gründe für die Verarbeitung vorliegen, die personenbezogenen Daten unrechtmäßig verarbeitet wurden oder die Löschung der Daten aufgrund anderer gesetzlicher Vorgaben vorgeschrieben ist.

Im Netz wird der Hauptanwendungsfall meist das Wegfallen oder Fehlen einer Verarbeitungsgrundlage sein. Denn personenbezogene Daten werden besonders oft auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO, also aufgrund eines berechtigten Interesses des Verantwortlichen verarbeitet. Hiergegen kann die betroffene Person einen Widerruf nach Art. 21 DSGVO einlegen, wenn sie der Auffassung ist, dass die Datenverarbeitung nicht mehr rechtmäßig ist. Regelmäßig kommt auch der Fall vor, dass eine Datenverarbeitung schon gar nicht rechtmäßig war, auch dann ist der Verantwortliche konsequenterweise verpflichtet, die personenbezogenen Daten zu löschen.

1 So schon Thinius, Google, vergiss mich (nicht)!, DFN-Infobrief Recht 10/2013; Thinius, Google, du musst mich vergessen!, DFN-Infobrief Recht 7/2014; Leinemann, Vergiss mein nicht…, DFN-Infobrief Recht 8/2016; Baur, Google weiß, was Du letzten Sommer getan hast, DFN-Infobrief Recht 4/2019; Tiessen, Schwamm drüber, Google, DFN-Infobrief Recht 10/2020.

Doch das Recht auf Löschung aus Art. 17 DSGVO gilt nicht ohne Beschränkungen. Absatz 3 der Vorschrift sieht insoweit Ausnahmen von der Löschpflicht des Verantwortlichen vor. Insbesondere wenn die Verarbeitung der personenbezogenen Daten für die Ausübung des Rechts auf freie Meinungsäußerung oder Information erforderlich ist, kann der Verantwortliche das Löschbegehren zurückweisen. Auch die Erfüllung rechtlicher Pflichten, Gründe des öffentlichen Interesses, bestimmte Archivzwecke oder die Durchsetzung von Rechtsansprüchen können das Recht auf Löschung beschränken.

Im Rahmen der Forderung nach einer Löschung sorgt für viele Streitigkeiten zwischen den Parteien regelmäßig die Ausübung des Rechts der freien Meinungsäußerung und Information. Denn in diesen Fällen läuft es meist auf eine umfangreiche Interessenabwägung hinaus, welche die Parteien denklogisch immer für sich selbst entschieden sehen. Aus diesem Grund schlagen diese Streitigkeiten besonders oft bei den obersten Bundesgerichten auf.

II. Sachverhalt

Das Verfahren hat seinen Ursprung schon im Jahr 2015. Der Kläger ist in der Finanzdienstleistungsbranche tätig und in diesem Bereich in verantwortungsvoller Position aktiv und Teilhaber von verschiedenen Gesellschaften. Die andere Klägerin ist Prokuristin einer dieser Gesellschaften.

2015 erschienen auf einer US-amerikanischen Webseite mehrere Artikel, welche die Geschäftspraktiken einige der Gesellschaften kritisierten. Anlass sei für das US-amerikanische Unternehmen, welches die Webseite betreibt, durch „aktive Aufklärung und Transparenz nachhaltig zur Betrugsprävention in Wirtschaft und Gesellschaft beizutragen“. Dabei verwendete das Unternehmen für einige der Beiträge Fotos von den Klageparteien. Diese Berichte und Fotos waren über Suchmaschinen zu finden, wenn man die Namen der beiden Unternehmer:innen bzw. die der Gesellschaften eingab.

Doch auch über die Webseite mit den Artikeln wurde wiederum negativ berichtet. So soll die kritische Berichterstattung nur dem Zweck dienen, dass Unternehmen mit den negativen Beiträgen erpresst werden. Demnach werden die Beiträge zunächst veröffentlicht, um anschließend von den Unternehmen ein Schutzgeld zu verlangen, damit die Veröffentlichungen wieder gelöscht werden bzw. eine Veröffentlichung weitere Artikel unterbleibt. Auch der Kläger und die Klägerin machen geltend, auf diese Art erpresst worden zu sein. Daher verlangten sie von Google als Verantwortliche für ihre Suchmaschine, die Auflistung dieser Beiträge und Fotos zu unterlassen, wenn die Namen der Klageparteien bzw. der Gesellschaften in die Suchmaschine eingegeben werden.
Google erklärte den beiden Unternehmer:innen dagegen, dass es nicht in der Lage sei, die Richtigkeit der Beiträge beurteilen zu können und nahm aus diesem Grund die geforderte Unterlassung der Auflistung nicht vor.

III. Verfahrensverlauf

Dieser Sachverhalt beschäftigte die deutsche und europäische Gerichtsbarkeit nun die letzten acht Jahre durch alle Instanzen hinweg.

1. Landgericht Köln

Die Klageparteien reichten ihre Klage vor dem Landgericht (LG) Köln ein. Dieses wies die Klage aber in seinem Urteil vom 22. November 2017 (Az. 28 O 492/15) größtenteils mit der Begründung ab, dass die Klageparteien nicht in ihren Rechten verletzt wurden. Insbesondere überwiege das Veröffentlichungsrecht von Google das Persönlichkeitsrecht der Klageparteien, da in den angezeigten Links nach Ansicht des Gerichts keine rechtsverletzenden Inhalte zu finden seien. Die Listung der Fotos in der Suche seien darüber hinaus als Bildnisse der Zeitgeschichte zulässig.

2. Oberlandesgericht Köln

Nach dem Urteil des LG Köln wandten sich die Klageparteien mit ihrer Berufung an das Oberlandesgericht (OLG) Köln. Dieses wies die Berufung mit Urteil vom 8. November 2018 (Az.: 15 U 178/17) vollumfänglich zurück und gab somit der Entscheidung des LG Köln in der Sache Recht. Insoweit treffe die Klageparteien die Pflicht nachzuweisen, dass die Inhalte der in der Suche angezeigten Links bzw. die dort enthaltenen Äußerungen in tatsächlicher und rechtlicher Hinsicht ihre Rechte offensichtlich verletzen. Dies sei den Klageparteien nach Ansicht des Gerichts nicht gelungen.

3. Bundesgerichtshof

Aufgrund dieser Entscheidung beschritten die Klageparteien den Weg zum BGH, um Revision gegen das Urteil des OLG Köln einzulegen. Doch aufgrund des Bezuges zum europäischen Datenschutzrecht des infrage stehenden Art. 17 DSGVO setzte der BGH das Verfahren mit Beschluss vom 27. Juli 2020 (Az. VI ZR 476/18) aus und legte dem EuGH zwei Fragen zur Auslegung des Art. 17 DSGVO im Wege des Vorabentscheidungsverfahrens vor.[2]

Der BGH wollte zum einen wissen, ob in der Abwägung der widerstreitenden Interessen berücksichtigt werden könne, ob die Klageparteien ein Vorabverfahren zur Überprüfung der Wahrheit der über sie erschienenen Beiträge durchgeführt haben und sie somit von der Möglichkeit, seine Behauptungen gerichtlich überprüfen zu lassen, Gebrauch gemacht haben. Praktisch würde dieses Vorabverfahren für Klagen dieser Art bedeuten, dass die Partei, welche die Unterlassung einer Auflistung in Suchergebnissen fordert, vor der Unterlassungsklage eine zusätzliche Feststellungsklage durchführen müsste. Nur wenn diese zum Ergebnis führt, dass die zu entfernende Information falsch ist, könnte das Verfahren auf Unterlassung beschritten werden.

Zum anderen fragte der BGH, inwiefern der Kontext der ursprünglichen Veröffentlichung innerhalb der Abwägung nach Art. 17 Abs. 3 lit. a DSGVO zu berücksichtigen sei, wenn der Suchdienstanbieter nur ein Vorschaubild mit Link, nicht aber den Titel der Website oder anderweitige Informationen der Ursprungsseite nennt.

Beide Fragen drehen sich letztlich darum, inwieweit die Suchanzeige und die verlinkte Website rechtlich getrennt voneinander betrachtet werden können.

4. Gerichtshof der Europäischen Union

Mit Urteil vom 8. Dezember 2022 (Az. C-460/20) beantwortete der EuGH auf die Fragen des BGH, dass Suchmaschinen wie Google Einträge aus ihren Ergebnissen löschen müssen, wenn sie nachweislich falsch sind. Doch hierfür brauche es keine richterliche Entscheidung. Es sei von den betroffenen Personen lediglich der Beweis hierzu erbringen, der vernünftigerweise verlangt werden kann. Der Suchmaschinenbetreiber selbst muss bei der Beweiserbringung nicht aktiv mitwirken.

Darüber hinaus stellte der EuGH klar, dass Google prüfen müsse, ob die gerügten Vorschaubilder für die Ausübung des Rechts auf freie Information durch die Internetnutzer erforderlich sind. Insbesondere sei zwischen Fotos zu unterscheiden, die in einem Artikel in ihrem ursprünglichen Kontext eingebettet seien und solchen Fotos, die nur in der Vorschauliste außerhalb des Kontexts angezeigt werden.

IV. Entscheidung des Bundesgerichtshofs

Auf Grundlage der Feststellungen des EuGHs entschied der BGH nun final auf das Klagebegehren der beiden Parteien mit Urteil vom 23. Mai 2023 (Az.: VI ZR 476/18)[3] und gab den Klageparteien teilweise in ihrer Revision Recht.

Der BGH bestätigte das vorinstanzliche Urteil des OLG Köln soweit, dass die Klageparteien ihrer, nun vom EuGH vorausgesetzten Beweispflicht, nicht ausreichend nachgekommen seien. Die bereitgestellten Informationen genügen nicht, um die offensichtliche Unrichtigkeit der aufgelisteten Beiträge feststellen zu können.

Doch bezüglich der Vorschaubilder entschied der BGH nun anders als das OLG Köln: Google wurde insoweit verpflichtet, die Vorschaubilder von den Suchergebnissen auszulisten. Die Anzeige ohne jeden Kontext sei im Rahmen der vorzunehmenden Interessenabwägung nicht gerechtfertigt.

V. Fazit und Auswirkungen für die Praxis

Die Urteile des EuGHs und des BGHs sind Teil einer umfangreichen gerichtlichen Ausgestaltung des Rechts auf Löschung. Dadurch, dass die DSGVO noch eine vergleichsweise junge Verordnung ist, sind viele Detailfragen bislang ungeklärt und sorgen in der Praxis für Rechtsunsicherheiten. Urteile wie diese schaffen nun wieder ein weiteres Stückchen Klarheit.

Im vorliegenden Fall lässt sich insbesondere festhalten, dass Suchmaschinenbetreibende dazu verpflichtet sind, Ergebnisse auszulisten, wenn diese nachweislich offensichtlich unrichtig sind. Doch eine eigene Ermittlungspflicht besteht dabei für die Suchmaschinenbetreibenden nicht. Es ist Sache der betroffenen

2 Hierzu auch Tiessen, Schwamm drüber, Google, DFN-Infobrief Recht 10/2020.

3 Zum Zeitpunkt der Bearbeitung liegt nur die Pressemitteilung des BGHs vor.

Personen, diese Nachweise zu führen. Dennoch muss der Aufwand hierfür angemessen bleiben. Fraglich bleibt, wie diese Angemessenheit im Einzelfall aussieht.
Darüber hinaus steht fest, dass das Recht am eigenen Bild überwiegt, wenn Vorschaufotos ohne jeden Zusammenhang in den Suchergebnissen gelistet werden. Für die Überprüfung, ob ein Bild rechtmäßig angezeigt wird, sind daher stets die zum Bild angezeigten Informationen heranzuziehen.

Diese Erkenntnisse haben auch für Mitglieder von Hochschulen und Forschungseinrichtungen Relevanz. Insbesondere wenn personenbezogene Daten in einem falschen Kontext oder Fotos aus privaten Bereichen des Lebens an die Öffentlichkeit gezogen werden, kann der Rechtsweg gegen den Suchmaschinenbetreibenden oftmals der erfolgversprechendste sein. Doch hierzu muss die betroffene Person den Nachweis führen können, dass die Informationen offensichtlich unrichtig sind.

Hier werden keine Daten gecloud

DSK stellt Positionspapier zur Nutzung von souveränen Clouds vor

Von Johannes Müller

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)[1] hat eine Stellungnahme zur Nutzung von souveränen Clouds veröffentlicht.[2] Hierzu nennt sie eine Vielzahl konkreter Kriterien, anhand derer Cloud-Anbieter und Anwender überprüfen können, ob ein spezifischer Cloud-Computing-Dienst souverän im Sinne ihrer Stellungnahme ist.

I. Souveräne Clouds als politisches Entwicklungsziel

Die Auslagerung von Computerressourcen, etwa in Form von Datenspeichern oder Softwareanwendungen, auf Cloud-Computing-Dienste über das Internet stellt einen integralen Bestandteil der derzeitigen Digitalisierung dar. Vorteile der Nutzung von Cloud-Computing-Diensten liegen unter anderem darin, dass die verwendete Cloud-Infrastruktur dynamisch an die eigenen Ansprüche angepasst werden kann. Besteht etwa kurzzeitig ein erhöhter Bedarf für zusätzlichen Speicherplatz, lässt sich dieser im benötigten Zeitraum flexibel anmieten, ohne dass dauerhafte Investitionen, beispielsweise in die Erweiterung des eigenen Rechenzentrums, notwendig sind. Ebenso bringen Cloud-Computing-Dienste den Vorteil mit sich, dass ein Zugriff auf die Anwendungen über Internetverbindung von nahezu jedem Gerät möglich ist.

Die Auslagerung von Ressourcen auf Cloud-Computing-Dienste birgt allerdings auch Risiken. Die Nutzung fremder IT-Infrastruktur kann mit einer Ungewissheit darüber einhergehen, welche Personen Zugriff auf die gespeicherten Daten oder die genutzte Software haben. Befinden sich die Server der Cloud im EU-Ausland, beispielsweise in den USA, besteht etwa das Risiko, dass ausländische Sicherheitsbehörden Zugriff auf die Daten erhalten. Daneben kommen aber auch zahlreiche Gefahren durch private Akteure in Betracht, etwa in Form eines Datendiebstahls durch einen Hackerangriff. Aufgrund dieser Gefahren gewinnt die Thematik der souveränen Clouds zunehmend an Bedeutung und wird auch auf politischer Ebene kritisch diskutiert. Die Anforderungen an eine souveräne Cloud sind bisher nicht fest definiert. In ihrer Stellungnahme nennt die DSK die Definition des Kompetenzzentrums Öffentliche IT, nach der „Digitale Souveränität" als „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können"[3] definiert wird. Daran anknüpfend beschäftigt sich die DSK in ihrer Stellungnahme mit unterschiedlichen Kriterien, die eine souveräne Cloud erfüllen soll. Diese Kriterien richten sich sowohl an Anbieter von Cloud-Diensten als auch deren Anwender. Insbesondere letztere sollen durch die Kriterien bei der Auswahl einer Cloud-Lösung unterstützt werden. Die Bewertung von souveränen Clouds erfolgt durch die DSK primär aus datenschutzrechtlicher Perspektive. So betont die DSK, dass eine souveräne Cloud alle Vorgaben des Datenschutzrechtes, sowohl aus der DSGVO als auch aus den bundes- und landesrechtlichen Regelungen einzuhalten hat. Eine souveräne Cloud soll hierüber hinausgehend jedoch nicht lediglich datenschutzkonform sein, sondern auch die zugrundeliegende Problematik grundlegend und nachhaltig lösen.

---

1 Vgl. zur Arbeit der DSK beispielhaft Müller, Datenschutz auf Rezept, DFN-Infobrief Recht 02/2023.

2 Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023. Kriterien für Souveräne Clouds, https://www.datenschutzzentrum.de/uploads/dsk/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf (zuletzt abgerufen am 15.06.2023).

3 Kompetenzzentrum Öffentliche IT, Digitale Souveränität, 3, https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t (zuletzt abgerufen am 15.06.2023).

Im Rahmen ihrer Stellungnahme nennt die DSK einerseits Muss-Kriterien, die eine souveräne Cloud zwingend zu erfüllen hat und darüber hinaus Soll-Kriterien, die zusätzliche Empfehlungen darstellen.

II. Nachvollziehbarkeit durch Transparenz

Die DSK beschäftigt sich zunächst mit dem Transparenzgrundsatz des Art. 5 Abs. 1 lit. a DSGVO. Diesem zu Folge hat eine Verarbeitung personenbezogener Daten in einer für die betroffene Person nachvollziehbaren Weise zu erfolgen. Demnach müssen Anbieter von Cloud-Diensten imstande sein nachzuweisen, dass die Datenverarbeitung nach den Vorgaben der DSGVO erfolgt. Im Rahmen eines transparenten Cloud-Angebots muss der Cloud-Anbieter dem Cloud-Anwender bereits vor Vertragsschluss eine Dokumentation zur Verfügung stellen, die Auskunft darüber gibt, welche externen Komponenten und Dienstleistungen im Rahmen des Cloud-Angebots eingesetzt werden und dass die Verarbeitung hierbei datenschutzkonform erfolgt. Zum Nachweis können etwa Vereinbarungen mit Dritten vorgelegt werden.
Zur Gewährleistung der Interoperabilität mit anderen Cloud-Systemen müssen Cloud-Anbieter die Anwender über die verfügbaren Schnittstellen und Möglichkeiten des Datenexports informieren. Zu den Transparenzanforderungen zählt die DSK auch die Pflicht der Anbieter nachzuweisen, wie sie in Zukunft einen dauerhaften und unabhängigen Betrieb des Angebots gewährleisten wollen. Als Empfehlungen für eine transparente Cloud-Nutzung nennt das Papier darüber hinaus den Einsatz von Open-Source-Software und offener Standards.

III. Datenhoheit und Kontrollierbarkeit

Essentiell für eine souveräne Cloud ist die Kontrollierbarkeit ihrer Nutzung, sodass betroffene Personen ihre Datenhoheit wahren können.
Um die Anforderungen an die Kontrollierbarkeit einer souveränen Cloud zu erfüllen, ist es erforderlich, dass die Anbieter der Cloud personenbezogene Daten ausschließlich im Rahmen von konkreten Weisungen verarbeiten. Innerhalb der Cloud-Nutzung muss zudem eine Trennung der unterschiedlichen Verarbeitungsvorgänge erfolgen. Ist eine physische Trennung nicht möglich, hat diese durch technische und organisatorische Maßnahmen zu erfolgen. Die Stellungnahme empfiehlt zudem, dass bei der Einschaltung von Unterauftragsverarbeitern die Anwender selbst möglichst weitgehend auf diese einwirken und auch einzelne Unterauftragsverarbeiter abwählen können.

Zu dem Kriterium der Datenhoheit zählt die DSK auch die Verhinderung von Zugriffsmöglichkeiten der Behörden von Drittländern. Die Anbieter haben sicherzustellen, dass ausschließlich Datenzugriffe möglich sind, die nach EU-, EWR- bzw. nationalem Recht zulässig sind. Hierfür genügen in der Regel keine vertraglichen Maßnahmen.
Um die Beherrschbarkeit der Daten sicherzustellen, müssen Rechte und Pflichten eindeutig vertraglich festgehalten werden. Es muss festgelegt werden, wie die Verletzung dieser Rechte und Pflichten sanktioniert wird. Die Sanktionen müssen ferner gerichtlich durchsetzbar sein.

Bezüglich des Anbietersitzes und des Verarbeitungsortes geht die Empfehlung über die datenschutzrechtlichen Pflichten hinaus. Die DSGVO sieht die Möglichkeit zur Übertragung personenbezogener Daten in Drittländer vor. Hingegen erfordert eine souveräne Cloud nach Ansicht der DSK eine Datenverarbeitung, die ausschließlich im Europäischen Wirtschaftsraum stattfindet.

IV. Offenheit

Ein weiteres Kriterium, welches der effektiven, nachprüfbaren und dauerhaften Einhaltung der datenschutzrechtlichen Pflichten von Cloud-Anbietenden dient, ist das der Offenheit. Zur Ausgestaltung ihrer Verarbeitungstätigkeiten sollen die Anwendenden eine Wahlmöglichkeit zwischen unterschiedlichen Cloud-Angeboten haben, um Abhängigkeiten zu vermeiden. Dazu sollen auch spätere Wechsel des Cloud-Angebots mit möglichst geringem Aufwand möglich sein.
Um diesem Kriterium gerecht zu werden, ist es notwendig, dass die Cloud-Angebote einfach zu ersetzen sind. Sie müssen insbesondere den Export aller betrieblich relevanten Daten und Objekte ermöglichen. Außerdem empfiehlt die DSK, den Anbietern souveräner Clouds ein hohes Maß an Kombinierbarkeit ihrer Lösungen zu ermöglichen und den Anwendern diesbezüglich angemessene Dokumentationen und Hilfsmittel bereitzustellen. Zum einen sollte die Einbindung externer IT-Systeme und -dienste in das Cloud-Angebot möglich sein. Zum anderen sollte das Cloud-Angebot selbst in andere Lösungen einzubinden sein. Hiermit geht die Möglichkeit einher, Teilkomponenten und -funktionen souveräner Cloud-Angebote zu nutzen, die für Anwender bestehen sollte.

Der Offenheit von Cloud-Angeboten kommt zudem zugute, wenn die souveräne Cloud in möglichst allen Bereichen eine Nutzung auf Basis von offenen Standards erlaubt. Nicht nur Dateiformate, sondern auch etwaige Schnittstellen und Protokollierungen sollten auf offenen Standards basieren. Allerdings sollte die Nutzung einer Cloud auch ohne spezifische Erweiterungen möglich sein. Darüber hinaus sollten souveräne Clouds bestenfalls vollständig auf Open-Source-Software basieren, um Anwendern bei Bedarf Einblick in die Umsetzung der Cloud-Plattform zu verschaffen. So könnten im Falle eines Angebotswechsels hilfreiche Informationen erlangt und – sofern die Plattform unter einer freien Lizenz steht – Teile der Umsetzung übernommen werden.

V. Vorhersehbarkeit und Verlässlichkeit

Um die Souveränität der Cloud-Angebote langfristig zu erhalten, müssen diese vorhersehbar und verlässlich sein. Dazu ist es notwendig, dass die Anbieter die Anwender frühzeitig über Strukturänderungen informieren, die sich negativ auf die Souveränität des Angebotes auswirken könnten. Weiterhin sind die Prinzipien des Art. 25 Abs. 1 und 2 DSGVO einzuhalten: Voreinstellungen von Cloud-Angeboten sind von den Anbietern stets datenschutzfreundlich zu wählen und Wechselwirkungen müssen transparent gemacht werden. Außerdem müssen Weiterentwicklungen möglichst modular erfolgen und – insbesondere im Falle sich ergebender datenschutzrechtlicher Risiken – möglichst auch abwählbar sein. Empfehlenswert ist zudem ein transparentes Geschäfts- und Finanzierungsmodell der Anbieter, damit sich die Seriosität und Rechtmäßigkeit des Modells überprüfen lässt. Um Änderungen nachvollziehen zu können, sollte sich die Transparenz zudem nicht auf das gegenwärtige Finanzierungsmodell beschränken. Damit die Weiterentwicklung, Änderung und Abkündigung von Eigenschaften für die Anwender eines Cloud-Angebots verlässlich und vorhersehbar ist, müssen diese in transparent dargelegten und planbaren Zyklen erfolgen. Außerdem bietet sich die Verwendung von Open-Source-Software wegen der notwendigen Prüffähigkeit von Cloud-Angeboten an, da diese Anwendern die Überprüfung der Qualität eines Angebots erlaubt. Wenn Anbieter ihre Public Clouds auch in einer souveränen Ausgestaltung anbieten, sollten sie mittelfristig Featureparität zwischen beiden Varianten anstreben, um einen schleichenden Druck zum Verzicht auf das souveräne Angebot zu verhindern. Wird Featureparität nicht geschaffen, sollte zumindest über die Unterschiede zwischen den Varianten transparent und neutral informiert werden.

VI. Regelmäßige Prüfung der Kriterien

Zum Schluss beschäftigt sich die DSK in ihrer Stellungnahme noch mit der Überprüfung der aufgestellten Kriterien. Ob und welche der genannten Kriterien ein Cloud-Angebot erfüllt, muss für Anwender prüf- und nachvollziehbar sein. Zum einen muss die Software deshalb grundsätzlich überprüfbar sein. Zum anderen muss sie auch tatsächlich regelmäßig – und spätestens bei einer Änderung der mit den Verarbeitungsvorgängen verbundenen Risiken – überprüft werden. Dazu bedarf es der Bereitschaft der Anbieter, an einer solchen Überprüfung aktiv mitzuwirken (vgl. Art. 28 Abs. 3 lit. h DS-GVO). Die Anbieter müssen also detaillierte Dokumentationen bereitstellen, auf Nachfragen antworten oder sich auch selbst an Vor-Ort-Überprüfungen beteiligen. Bestenfalls nutzen sie Zertifizierungsverfahren, mit denen die Einhaltung der DSGVO und der Kriterien der DSK nachgewiesen werden kann.

VII. Relevanz für wissenschaftliche Einrichtungen

Die Stellungnahme der DSK weist eine hohe Relevanz für wissenschaftliche Einrichtungen auf. Wie allen Veröffentlichungen der DSK kommt auch der vorliegenden Stellungnahme keine verbindliche Wirkung zu.[4] Aufgrund der Zusammensetzung der DSK aus allen Datenschutzbeauftragten der Länder und dem Bundesdatenschutzbeauftragten ist ihren Empfehlungen jedoch stets ein hohes Gewicht beizumessen. Befinden sich Universitäten oder andere wissenschaftliche Einrichtungen im Auswahlprozess eines Cloud-Computing-Dienstes, bieten die aufgestellten Kriterien eine starke Orientierungshilfe, um festzustellen, ob ein Cloud-Dienst die gängigen Anforderungen an die Souveränität erfüllt. Wissenschaftliche Einrichtungen sollten diese Kriterien berücksichtigen und lediglich souveräne Cloud-Computing-Dienste einsetzen. Einen großen Mehrwert bietet das Positionspapier der DSK insbesondere, weil eine Vielzahl der Kriterien konkret überprüfbar und umsetzbar sind und sich die Empfehlung damit nicht lediglich auf die Wiedergabe der Rechtslage beschränkt.

4 Vgl. Müller, Datenschutz auf Rezept, DFN-Infobrief Recht 02/2023.

Kurzbeitrag: Patient Patentrecht

Vorschlag der EU-Kommission für neue Patentvorschriften

von Klaus Palenberg

Nachdem im Juni das europäische Einheitspatentsystem in Kraft getreten ist, möchte die Europäische Union nun auch weitere Bereiche des Patentrechts regeln. Hierzu hat die EU-Kommission einen Vorschlag für neue Patentvorschriften veröffentlicht. Im Fokus der neuen Verordnungen soll die Nutzung von Standardessenziellen Patenten (SEP) durch kleine und mittlere Unternehmen (KMU), sowie die Nutzung von patentgeschützten Produkten in Krisenzeiten stehen.

I. Anknüpfungspunkt

Geistiges Eigentum spielt eine sehr wichtige Rolle für die europäische Wirtschaft. So erwirtschaften die hiervon erfassten Unternehmen laut einer entsprechenden Pressemitteilung der Europäischen Kommission fast die Hälfte des gesamten Bruttoinlandprodukts der EU und machen über 90 Prozent der Exporte aus. Aber auch innerhalb der EU sind patentintensive Branchen ein, mit einem Anteil am Intra-EU-Handel von fast 76 Prozent in den Jahren 2017-2019, sehr bedeutender Wirtschaftszweig.
Am 01. Juni ist in diesem Zusammenhang das System des Einheitspatents in Kraft getreten. Damit ist ein europäisches Patent mit einheitlicher Wirkung in allen teilnehmenden EU-Mitgliedstaaten und einem gemeinsamen Rechtsschutz vor dem Einheitlichen Patentgericht eingeführt worden. Dieses System soll ergänzt werden durch den vorgeschlagenen Entwurf der EU-Kommission für mehrere neue Verordnungen.

II. Regelungsbereiche

Standardessentielle-Patente sind Patente, die wesentlich für die Umsetzung einer technischen Norm sind. Ohne diese kann in dem entsprechenden Bereich faktisch nicht gewirtschaftet werden. Ein bekanntes Beispiel ist etwa der Mobilfunkstandard „5G“. Um an diesem Standard teilnehmen zu können, müssen die entsprechenden SEP genutzt werden. Dadurch entstehen jedoch auf Seiten der Patentinhaber der SEP faktische Monopole, denen derzeit durch die Verpflichtung begegnet werden soll, diese Patente zu fairen, angemessenen und diskriminierungsfreien Bedingungen (FRAND-Bedingungen) zu lizenzieren. Dieses System wird jedoch von fehlender Transparenz, Vorhersehbarkeit und fortdauernden Rechtsstreitigkeiten begleitet.

An dieser Stelle sollen die neuen Regelungen eingreifen und sicherstellen, dass SEP trotz der genannten Schwierigkeiten durch europäische Unternehmen nutzbar bleiben. Hierzu soll ein SEP-Register eingeführt werden und auf Grundlage von Sachverständigengutachten zu SEP-Gesamtlizenzgebühren faire und angemessene Preise ermöglicht werden. Diese FRAND-Bestimmungen (fair, reasonable and non-discriminatory) sollen zudem durch Schlichtungen anstatt von aufwändigen Gerichtsverfahren überprüft werden können. Zudem sollen KMU bei der Lizensierung durch das Amt der Europäischen Union für geistiges Eigentum (EUIPO) unterstützt werden.

Ein weiterer Regelungsgegenstand soll die Zwangslizensierung von Patenten sein. In Krisenzeiten soll es damit staatlichen Stellen ermöglicht werden auch gegen den Willen der Patentinhaber bestimmte patentierte Erfindungen zu nutzen. Damit soll der derzeitige Flickenteppich an verschiedenen nationalen Regelungen beseitigt werden, um für mehr Rechtssicherheit bei den Patentinhabern zu sorgen und aktuelle EU-Kriseninstrumente zu ergänzen.

Als dritter Baustein soll ein ergänzendes Schutzzertifikat (SPC) als eigenes Recht des geistigen Eigentums eingeführt werden, das die Laufzeit eines Patents um bis zu fünf Jahre verlängern kann. Für Human- oder Tierarzneimittel und Pflanzenschutzmittel soll hiermit das Einheitspatent ergänzt und ein einheitlicher Schutz in der EU gewährleistet werden.

III. Ausblick und Folgen

Der Entwurf geht nun an das Europäische Parlament und den Rat der Europäischen Union, um im weiteren Lauf der Gesetzgebung angenommen zu werden.
Mit diesen Regelungen wird ein weiterer Schritt hin zu einem vereinheitlichten Schutz von Immaterialgüterrechten in Europa gegangen. Damit soll insbesondere die Innovationskraft und Wettbewerbsfähigkeit der europäischen Wirtschaft gestärkt werden. Auf der anderen Seite sollen den staatlichen Stellen aber auch Zugriffsmöglichkeiten an die Hand gegeben werden, um in Krisenzeiten nicht allein vom guten Willen der Patentinhaber abhängig zu sein. Dies ist eine bedeutende Lehre aus der Pandemie und der großen Abhängigkeit von den Impfstoffherstellern. Im Gegenzug wird diesen Branchen wiederum eine Schutzzeitverlängerung durch das SPC eingeräumt.

Gerade für Produkte, die für den gesamten europäischen Markt entwickelt werden, vereinfacht sich die Anmeldung entsprechender Patente bereits durch das Einheitspatent sehr. Mit den vorgeschlagenen Regelungen wird dieses nun dahingehend flankiert, dass auch andere Aspekte vereinheitlicht werden. Dies schafft insoweit mehr Rechtssicherheit und gleiche Wettbewerbsbedingungen im europäischen Raum. Auf der anderen Seite müssen die zahlreichen einzelstaatlichen Regelungssysteme in den ersten Jahren zunächst aufeinander abgestimmt werden. Somit wird diese Rechtssicherheit vermeintlich erst nach den ersten Gerichtsentscheidungen auf der Basis der einheitlichen Regelungen eintreten.

Jedenfalls in Hinblick auf SEP vereinfacht sich die Nutzung auch für die Wissenschaft allein schon durch die ausdrückliche gesetzgeberische Anerkennung der FRAND-Bedingungen in Bezug auf SEP. Es bleibt aber abzuwarten, wie die Sachverständigengutachten für die Lizenzgebühren ausfallen. Für wissenschaftliche Einrichtungen oder deren Mitarbeitende, die Inhaber von SEP sind, könnten sich durch das neue System aber auch Nachteile, insbesondere finanzieller Natur, ergeben.

Impressum

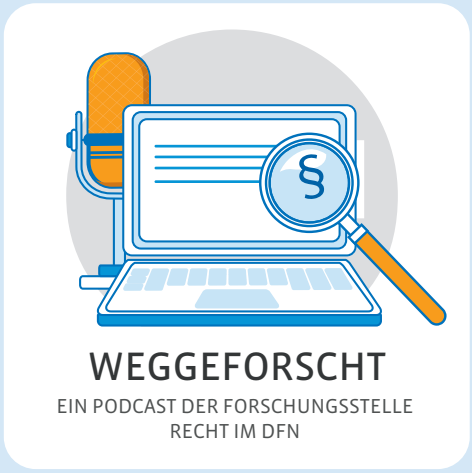
Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz.

Herausgeber

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

Redaktion

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der WESTFÄLISCHEN WILHELMS-UNIVERSITÄT, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung
Unter Leitung von Prof. Dr. Thomas Hoeren
Leonardo-Campus 9
D-48149 Münster
E-Mail: recht@dfn.de



Podcast der Forschungsstelle Recht im DFN

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

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

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