„Weggeforscht“ der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht

12 / 2023
Dezember 2023

Geschenke verpacken leicht gemacht: Transparenz ist in!

Die Transparenzdatenbank des Digital Services Act ist jetzt online

von Nicolas John

Soziale Netzwerke sind nicht mehr wegzudenken. Für das Teilen von Urlaubserinnerungen mit Familie und Freunden, das Bewerben von Produkten, die öffentliche Teilnahme an politischen Diskussionen oder das Erlangen von Informationen aus aller Welt – diverse Plattformen stillen die unterschiedlichen Bedürfnisse ihrer Nutzer:innen. Es ist unbestreitbar, dass soziale Netzwerke viele positive Facetten aufweisen. Doch wo Licht ist, ist auch Schatten: Hetzer, Verschwörungstheoretiker oder organisierte Desinformationskampagnen finden in den gleichen sozialen Netzwerken ihre Opfer. Die Europäische Union (EU) will mit dem Digital Services Act (DSA) für mehr Kontrolle und Transparenz sorgen. Als Teil hiervon ist nun die Transparenzdatenbank online gegangen.

I. DSA – Ein Überblick

Zu der Sammlung des scheinbar unerschöpflichen Vorrates der EU-Kommission an Gesetzesentwürfen im Rahmen der europäischen Digitalstrategie gehört seit Ende des Jahres 2022 mit seinem Inkrafttreten auch der DSA.[1] Durch diese Regulierung auf europäischer Ebene soll vor allem die Rechtsdurchsetzung im Internet gegen Hate Speech, Desinformation oder Verbrauchertäuschung verbessert werden. Große Online-Plattformen wie Suchmaschinen oder soziale Netzwerke werden daher zu mehr Schutz und Transparenz für Verbraucher:innen verpflichtet. Durch das Inkrafttreten des DSA wurde so ein einheitlicher, europaweiter Rechtsrahmen für den Verbraucherschutz und für die Haftung und Sicherheit auf digitalen Plattformen oder für digitale Dienste und Produkte geschaffen. Als unmittelbar geltende Verordnung löst er die bereits 20 Jahre alten Vorschriften der eCommerce-Richtlinie ab. Durch den DSA wurde außerdem auf eine zunehmende Zersplitterung der Vorschriften in den einzelnen Mitgliedstaaten reagiert. Einige Normen des DSA entfalten dabei bereits seit dem 16. November 2022 Geltung, vollständig verbindlich für alle betroffenen Betreibenden ist der Digital Services Act jedoch erst ab dem 17. Februar 2024.
Der Regelungsinhalt des DSA lässt sich maßgeblich in zwei große Kategorien einteilen. Zunächst gibt es die – dem deutschen Telemediengesetz weitgehend entsprechende – Haftungsprivilegierung für Vermittlungsdienste. Für diese sog. Internetzugangsdienste gilt der Grundsatz, dass ohne Kenntnis der Rechtswidrigkeit von Inhalten eine Haftung nicht in Frage kommt. Auf der anderen Seite werden durch den DSA umfassende Sorgfalts- und Transparenzpflichten normiert, die von den Diensteanbietenden (z.B. soziale Netzwerke, Suchmaschinen oder Online-Marktplätze) bei der Moderation von Inhalten und der Beschränkung von Nutzer:inneninhalten beachtet werden müssen.

Kurzum, selbsterklärtes Ziel des DSA ist, „offline“ geltende Vorgaben ebenbürtig in der digitalen Welt zu regulieren und durchsetzen zu können.

1 Siehe dazu Gielen, Digital Services Act: Das Plattformgrundgesetz?, DFN-Infobrief Recht 3/2021; Rennert, Brüssel reguliert das schon, DFN-Infobrief Recht 6/2022; Tech, Datenstaat oder Datensalat, DFN-Infobrief Recht 8/2023.

II. Die DSA-Transparenzdatenbank

Auch wenn der DSA erst ab dem 17. Februar 2024 vollständig Geltung erlangt, müssen schon bereits 17 sog. sehr große Plattformen und Suchmaschinen mit mehr als 45 Millionen Nutzer:innen pro Monat in der EU erste verpflichtende Vorgaben umsetzen. Erfasst werden hier u. a. Unternehmen wie Amazon, X (ehemals Twitter), TikTok, Google oder Zalando.

Von zentraler Bedeutung sind für die Betreibenden der sehr großen Plattformen die neu eingeführten Transparenzregeln und Beschwerdemöglichkeiten der Nutzer:innen. Wenn Nutzer:innen auf einer Plattform rechtswidrige Inhalte veröffentlichen und die Betreibenden davon Kenntnis erlangen, müssen diese Inhalte von den Betreibenden moderiert werden. Die davon betroffenen Personen müssen nach einer Entscheidung der Betreibenden über den Umgang mit dem Inhalt eine Begründung für etwaige Eingriffe oder Löschungen erhalten, um ggf. gegen sie vorgehen zu können. Auf diese Weise soll willkürlichen Entscheidungen durch die Plattformbetreibenden entgegengewirkt werden.
Neben dieser umfassenden Begründungspflicht der Betreibenden geht der DSA noch einen Schritt weiter. Die Begründungen für das Einschreiten gegen gemeldete Inhalte sollen nicht nur die betroffenen Nutzer:innen erhalten, sondern darüber hinaus in einem öffentlichen Online-Register[2] gesammelt werden. Grundlage für diese sog. Transparenzdatenbank ist Art. 24 Abs. 5 DSA, der deren Errichtung fordert. Die Betreibenden müssen danach ihre Entscheidungen sowie die dazugehörige Begründung an die Kommission übermitteln, wobei die zu übermittelnden Informationen für die Transparenzdatenbank keine personenbezogenen Daten enthalten dürfen.

Das Ziel der Datenbank erläutert Erwägungsgrund 66 DSA. Demnach soll die Datenbank „für Transparenz […] sorgen und die Kontrolle über die Entscheidungen von Anbietern von Online-Plattformen über die Moderation von Inhalten sowie die Überwachung der Verbreitung rechtswidriger Inhalte im Internet […] ermöglichen". Es gehe dagegen nicht darum, dass einzelne Entscheidungen durch die Schaffung der Transparenzdatenbank revidiert werden können.

Im Vordergrund steht die Durchsuchbarkeit der Moderationen und ihrer Begründungen. Dafür bietet die derzeitige Beta-Version der Datenbank eine Suchfunktion an. Mithilfe weiterer Einstellungsoptionen ist es möglich, nach eingetragenen Plattformen zu suchen, bestimmte Gründe der Moderation zu umfassen sowie die Art der Moderation oder Stichwörter in die Suche aufzunehmen. Darüber hinaus kann die Suche bezüglich privater oder öffentlicher Accounts, dem Geltungsbereich der Entscheidung, der Art des Inhalts, dem Automationsgrad der Entscheidung und des Zeitraums spezifiziert werden. Die gefundenen Informationen können anschließend als .csv-Datei heruntergeladen werden.[3] In Zukunft ist auch eine Visualisierung der Statistiken geplant, sodass z.B. Beeinflussungskampagnen mit gefälschten Profilen erkannt werden können. Zum Zeitpunkt dieser Recherche finden sich ca. 239 Mio. Einträge in der Datenbank, davon z. B.ca. 59 Mio. Einträge für TikTok, ca. 14 Mio. für Facebook oder 5,7 Mio. für Google Maps.

Im Übrigen ist der Source Code der Plattform öffentlich zugänglich.[4] Dies soll einerseits für eine tiefergehende Transparenz der Plattform selbst sorgen und andererseits dazu ermutigen, selbst eine maschinelle Auswertung der Daten vorzunehmen.

Wer sich mit den Möglichkeiten der Datennutzung und Auswertung der Daten auseinandersetzen möchte, kann durch die Dokumentation der Kommission detaillierte Informationen erhalten.[5] Die Dokumentation erläutert den Aufbau der enthaltenen Datensätze. Danach wird z. B. jeder eingetragenen Begründung ein sog. Platform Unique Identifier (PUID) zugeordnet. Diese PUID wird von der jeweiligen Plattform zugewiesen und dient z. B.der Verknüpfung mit einer spezifischen URL.

Insgesamt widmet sich die Dokumentation in sechs Abschnitten den Erklärungen zu den Dateneinträgen. Dazu gehören die Erläuterung der in der DSA-Transparenzdatenbank gespeicherten Informationen, die Vorlage klarer und spezifischer Erklärungen, die Informationen über die Art der auferlegten Beschränkung(en), der räumliche Geltungsbereich und die Dauer der Beschränkung, die Angaben zu den Tatsachen und Umständen, auf die sich die Entscheidung stützt, den Informationen über den Einsatz

2 In der Beta derzeit abrufbar unter https://transparency.dsa.ec.europa.eu/ (zuletzt abgerufen am 20.10.2023).

3 Wobei derzeit nur die ersten 10.000 Suchergebnisse auf der Webseite angezeigt werden und nur die ersten 1.000 Suchergebnisse als .csv-Datei heruntergeladen werden können.

4 Abrufbar auf GitHub https://github.com/digital-services-act/transparency-database (zuletzt abgerufen am 20.10.2023).

5 Abrufbar unter https://transparency.dsa.ec.europa.eu/page/documentation (zuletzt abgerufen am 25.10.2023).

automatisierter Mittel und die gesetzlichen oder vertraglichen Gründe, auf die sich die Entscheidung stützt.

III. Was bedeutet der DSA für die Forschung?

Die Transparenzmaßnahmen des DSA führen nicht nur zur Kontrolle der Maßnahmen durch die Allgemeinheit, sondern können durch die Sammlung der Moderationsdaten auch der Wissenschaft und Forschung dienen. Insoweit überrascht es nicht, dass in Erwägung gezogen wird, der Transparenzdatenbank in ihrer finalen Version auch eine Anwendungsschnittstelle (API) für Forschungszwecke hinzuzufügen. Die Kommission fordert hierfür in ihren Frequently Asked Questions (FAQ) ausdrücklich Feedback und Vorschläge für die Ausgestaltung einer solchen Schnittstelle. Hierfür dient das Feedback-Formular.[6]

Doch der DSA sorgt für Forschungszwecke nicht nur bei der Transparenzdatenbank für neue Möglichkeiten. Insoweit sieht Art. 40 DSA für Forschende einen Zugang zu den Daten der Plattformen vor. Die Daten sollen nach Absatz 4 „ausschließlich [zum] Zweck der Durchführung von Forschungsarbeiten, die zur Aufspürung, zur Ermittlung und zum Verständnis systemischer Risiken in der Union“ dienen. Unter diesen Risiken versteht der DSA unter anderem die Verbreitung rechtswidriger Inhalte, nachteilige Auswirkungen auf die Grundrechte, nachteilige Auswirkungen auf die gesellschaftliche Debatte oder Wahlprozesse oder auch nachteilige Auswirkungen in Bezug auf geschlechtsspezifische Gewalt sowie den Schutz der öffentlichen Gesundheit und von Minderjährigen.[7]

Nach Erwägungsgrund 95 DSA sollen daher sehr große Online-Plattformen oder sehr große Online-Suchmaschinen unter anderem „Archive für Werbung, die auf ihren Online-Schnittstellen angezeigt [werden], öffentlich zugänglich machen, um die Aufsicht und die Forschung zu neu entstehenden Risiken im Zusammenhang mit der Online-Verbreitung von Werbung zu unterstützen; dies betrifft etwa rechtswidrige Werbung oder manipulative Techniken und Desinformation mit realen und absehbaren negativen Auswirkungen auf“ die oben genannten Schutzgüter.

Der Zugang wird Forschenden vom sog. „Koordinator für digitale Dienste“ nur unter bestimmten Voraussetzungen zur Verfügung gestellt.[8] Wer in Deutschland die Rolle des Koordinators wahrnehmen soll, ist derzeit noch offen. Um Zugang erhalten zu können, müssen die Forschenden unter anderem an eine Forschungseinrichtung angeschlossen sein, die nicht gewinnorientiert agiert oder im Auftrag des öffentlichen Interesses tätig ist. Darüber hinaus dürfen keine kommerziellen Interessen verfolgt werden und die Forschenden müssen die Finanzierung ihrer Forschung offenlegen. Schließlich müssen sie Anforderungen an die Datensicherheit erfüllen können, die Notwendigkeit der Daten für ihre Forschungstätigkeit nachweisen, dem oben beschriebenen Forschungszweck entsprechen und sich dazu verpflichten, die Forschungsergebnisse nach Abschluss der Forschungsarbeiten innerhalb eines angemessenen Zeitraums kostenlos öffentlich zugänglich zu machen.[9]

Neben diesen Voraussetzungen muss der Zugriff auf die Daten stets unter Berücksichtigung der Interessen der Betreibenden und Nutzer:innen erfolgen. Daher haben die Betreibenden die Möglichkeit, einem Zugangsersuchen nicht vollumfänglich zu entsprechen. Dazu müssen besondere Gründe vorliegen, z. B. eine Verminderung der Sicherheit oder des Schutzes vertraulicher Informationen wie Geschäftsgeheimnisse.[10]

Mit diesen Zugangsmöglichkeiten soll die Transparenz neben der Transparenzdatenbank weiter erhöht werden und zur sicheren Nutzung der Plattformen beitragen. Die Wissenschaft und Forschung spielt daher eine zentrale Rolle in der Transparenzoffensive der EU. Aus diesem Grund wird der Zugang der Forschenden derzeit viel diskutiert. Ein kürzlich vom Weizenbaum-Institut

6 Abrufbar unter https://transparency.dsa.ec.europa.eu/feedback (zuletzt abgerufen am 26.10.2023).

7 Art. 34 DSA.

8 Siehe zur Rolle des „Koordinators für digitale Dienste“: Gielen, Digital Services Act: Das Plattformgrundgesetz?, DFN-Infobrief Recht 3/2021.

9 Art. 40 Abs. 8 DSA.

10 Art. 40 Abs. 6, Abs. 7 DSA.

Berlin veröffentlichtes Paper stellt z. B. 20 Forderungen für den Zugang zu den Daten für Forschende an die Politik.[11] Insbesondere der schnelle Zugang zu den Daten und finanzielle Anreize für die Plattformbetreibenden stehen im Zentrum der Forderungen.

IV. Fazit

Ob der DSA die gewünschte Wirkung für eine sicherere Nutzung von Plattformen und eine Verbesserung der Transparenz erzielen kann, wird sich erst in den kommenden Jahren zeigen. Allerdings zeigt die Einrichtung der Transparenzdatenbank, dass der DSA schon kurz nach Inkrafttreten seine ersten Früchte trägt. Auch die anhaltende Debatte um die Bedingungen des Datenzugangs offenbart die Bedeutung des Verständnisses der Risiken, welche von den Plattformen ausgehen können. Je breiter der Datenzugang am Ende gestaltet ist, desto wirksamer und effizienter kann die wissenschaftliche (und auch journalistische) Analyse über die Auswirkungen der Plattformen auf die Gesellschaft durchgeführt werden. Die Transparenzdatenbank ist hierfür ein wichtiger Schritt. Dennoch dürfen die Datenzugänge nicht missbräuchlich genutzt werden können. Die Sicherstellung der Rechte und Interessen der Plattformbetreibenden und Nutzer:innen müssen gegen die Forderungen der Wissenschaft stets abgewogen werden.

11 Klinger/Ohme, Was die Wissenschaft im Rahmen des Datenzugangs nach Art. 40 DSA braucht, abrufbar unter https://doi.org/10.34669/WI.WPP/8.1 (zuletzt abgerufen am 26.10.2023).

All I want for Christmas is Good Press

Die nationale Pressefreiheit auf dem Prüfstand

von Johanna Voget

Das Institut der freien Presse ist einer der Grundpfeiler unserer Demokratie. Weltweit sind jedoch besorgniserregende Entwicklungen zu beobachten. Journalist:innen werden angegriffen oder gar inhaftiert. Medienhäuser verbreiten Fake-News, missachten zusehends die Anforderungen an eine zulässige Berichterstattung oder tragen dazu bei, dass populistische und radikale Gesinnungen in der Gesellschaft zunehmen. Dieser Beitrag widmet sich den relevanten Problemen rund um Presse und Medien sowie dem Umgang des europäischen und nationalen Gesetzgebers und der Gerichte diesbezüglich.

I. Gefahren für Presse und Meinungsvielfalt

Auf der einen Seite wächst die Besorgnis um die Sicherheit der Medienschaffenden in Deutschland und weltweit. Zum Welttag der Pressefreiheit (3. Mai) hat die Menschenrechtsorganisation Reporter ohne Grenzen (RSF) wieder die Rangliste der Pressefreiheit aktualisiert. Deutschland liegt hier nur noch auf Platz 21, und ist damit das dritte Jahr in Folge abgestiegen.[1]

Der Grund hierfür ist die zunehmende Gewalt gegen Journalist:innen. Im Jahr 2022 wurden insgesamt 103 körperliche Angriffe auf Reporter und Medienschaffende dokumentiert, die sich hauptsächlich auf Versammlungen ereigneten. Mangels systematischer Erfassung ist darüber hinaus von einer hohen Dunkelziffer auszugehen. In anderen Ländern droht Journalist:innen bei regierungskritischer Berichterstattung eine Haftstrafe oder sogar der Tod.

Auf der anderen Seite wird aber auch immer häufiger Kritik an einigen Blättern und Formaten geübt: die Pressefreiheit werde überspannt und die Berichterstattung entspreche zunehmend nicht mehr den Anforderungen an den Pressekodex, sei also unwahrheitsgemäß, populistisch, radikal und stimmungsmachend. Daneben häufen sich auch die Zahlen gerichtlicher Verfahren gegen die Inhalte der Berichterstattung der Presse.

Beide Problemfelder werden noch dadurch verstärkt, dass die Digitalisierung die Medienlandschaft verändert: Kaum jemand liest heutzutage tatsächlich noch Printausgaben, sondern verwendet die neuen Informationskanäle über das Internet. Vorwiegend werden hierbei nicht die Websites der ursprünglichen Medienschaffenden verwendet, sondern soziale Netzwerke genutzt, die sich wiederum im Machtbereich einiger weniger Plattformen befinden.

Hier nehmen auch die psychischen Angriffe auf Medienschaffende unter dem Deckmantel der Anonymität immer mehr zu. Dem gegenüber steht die Zunahme der Verbreitung von schlecht recherchierten Fakten, stimmungsmachenden Fake-News und dem Kampf um Leser:innen durch Methoden wie Clickbaiting (Klickköder).

II. Maßnahmen zum Schutz von Presse- und Medienschaffenden

Um die Gefahren für Medienschaffende zu bekämpfen werden aktuell auf nationaler und europäischer Ebene einige Gesetzgebungsvorhaben auf den Weg gebracht, die im Folgenden näher beleuchtet werden sollen.

1 https://www.zdf.de/nachrichten/panorama/pressefreiheit-rangliste-ranking-deutschland-100.html (zuletzt abgerufen am 31.10.2023).

1. Gesetz gegen digitale Gewalt

Das Gesetzgebungsvorhaben widmet sich den Persönlichkeitsverletzungen im digitalen Raum (sog. digitale Gewalt).[2] Ziel ist also der Schutz und die Schaffung von Abwehrmöglichkeiten für Betroffene von Hass und Hetze im Internet.
Dazu hält das Eckpunktepapier der Bundesregierung folgende Maßnahmen bereit: Zunächst sollen private Auskunftsverfahren gestärkt werden, indem der Anwendungsbereich erweitert und das Verfahren effektiver ausgestaltet wird. Des Weiteren sieht der Vorschlag die Einführung eines Anspruchs auf eine richterlich angeordnete Accountsperre vor. Zuletzt sieht der Entwurf die Erleichterung der Zustellung durch die Pflicht zur Benennung eines inländischen Zustellungsbevollmächtigten, die bislang im NetzDG geregelt war, vor.
RSF empfiehlt als Reaktion auf den Vorschlag, Medienschaffende explizit als zu schützende Berufsgruppe in dem Gesetz gegen digitale Gewalt zu nennen.

An dem Entwurf wird jedoch auch viel Kritik geübt. Teilweise werden negative Auswirkungen auf die Meinungsfreiheit befürchtet, da nicht nur Beleidigungen und Drohungen unter die Regelungen fallen sollen, sondern auch „Schädigungen durch wahrheitswidrige Nutzerkommentare“, womit z.B. Online-Bewertungen von Gastronomie, Ärzten oder Hotels erfasst werden. Auch die Wirkung der Accountsperren ist umstritten, weil die blockierten Personen sich schließlich jederzeit unter neuem Namen erneut auf den Plattformen anmelden können.

2. European Media Freedom Act (EMFA)

Im September letzten Jahres legte die Kommission ihren Vorschlag für die Europäische Medienregulierung vor. Hintergrund des Tätigwerdens der EU ist vor allem die mangelnde politische Unabhängigkeit der Medien. Der EMFA nimmt daher alle Anbieter von Mediendiensten in der EU in die Pflicht und sieht Regelungen vor, die alle Redaktionen und Medienhäuser in ihrer Kernarbeit betreffen. Die Kommission will hiermit Medienpluralismus und -freiheit gewährleisten.[3] Überwacht werden soll die Einhaltung der Verordnung durch ein neu eingerichtetes „Europäisches Gremium für Mediendienste“.

Ob der Vorschlag jedoch tatsächlich zur Verabschiedung und Umsetzung gelangt, ist aus einem wesentlichen Grund sehr fraglich: Es bestehen Zweifel an der Kompetenz der Union zur Regelung der Materie. Die Kulturklausel des Art. 167 AEUV statuiert, dass jegliche kulturellen Angelegenheiten der ausschließlichen Regelungskompetenz der Mitgliedsstaaten unterfallen. Die EU bemüht daher die Binnenmarktkompetenz zur Begründung ihrer Zuständigkeit für einen Rechtsakt im Bereich der Medienregulierung.

3. Anti-SLAPP Richtlinie

Neben dem Vorschlag des EMFA veröffentlichte die Kommission im April 2022 den Entwurf einer sog. „Anti-SLAPP Richtlinie“. Die Forschungsstelle Recht berichtete bereits in einer Podcastfolge im vergangenen Jahr zu dem Vorhaben der EU, Journalist:innen und Medienschaffende auch prozessual mehr zu unterstützen. Dahinter stehen die sog. „Strategic Lawsuits against Public Participation“, oder anders gesagt: Einschüchterungsklagen gegen die Berichterstattung.[4] Mit diesem Rechtsakt sollen also Personen, die sich für den Schutz von öffentlichen Interessen einsetzen, vor offenkundig unbegründeten oder missbräuchlichen Gerichtsverfahren geschützt werden.

4. Digital Services Act (DSA)

Auch der DSA[5] soll durch die Regulierung von rechtwidrigen Inhalten und Desinformation Journalist:innen schützen.
Die in der Verordnung erwähnten Plattformen und Betreiber sozialer Netzwerke unterliegen danach einer Reihe von besonderen Verpflichtungen wie Melde- und Abhilfeverfahren für sog. illegale Inhalte (Art. 14 DSA). Unter den Begriff der illegalen Inhalte fallen beispielsweise illegale Hassreden, terroristische Inhalte oder Inhalte, die sich auf eine rechtswidrige Tätigkeiten beziehen, wie etwa die Darstellung von Kindesmissbrauch oder

2 https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Digitale_Gewalt_Eckpunkte.pdf;jsessionid=FB0D99815AF9EBAF7D383ADB9D9ACE2A.1_cid289?__blob=publicationFile&v=2 (zuletzt abgerufen am 31.10.2023).

3 Kraetzig, NJW 2023, 1485.

4 Mann, NJW 2022, 1358 ff.

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

die nicht einvernehmliche Verbreitung privater Bilder. Außerdem sind die Adressaten der Verordnung zur Meldung von Straftaten verpflichtet (Art. 15a DSA). Ziel des DSA ist damit die europäische Vereinheitlichung der Regeln für digitale Dienste als Mittel zur Bekämpfung rechtswidriger Inhalte und Desinformation.

III. Grenzen zulässiger Berichterstattung

So grundlegend und wichtig die Pressefreiheit auch ist – sie kann nicht uneingeschränkt zulasten des Einzelnen wirken. Neben den Fake-News über Tatsachen, werden immer wieder Personen Opfer von unwahrer Berichterstattung. In diesem Teil des Beitrags soll daher aufgezeigt werden, wie den Interessen beider Parteien Rechnung getragen werden kann und welche Grenzen die Pressefreiheit durch das allgemeine Persönlichkeitsrecht erfährt.

1. Kollision zwischen Pressefreiheit und allgemeinem Persönlichkeitsrecht

Bei der Prüfung, ob eine Persönlichkeitsrechtsverletzung durch die Berichterstattung erfolgt ist, ist stets eine Interessenabwägung im Einzelfall geboten. Bei der Frage nach der Schwere des Eingriffs ist neben dem konkreten Inhalt der Berichterstattung, seiner Form und dem Verbreitungsgrad insbesondere danach zu differenzieren, in welche Sphäre des Betroffenen die Berichterstattung eingreift. Hierbei ist zwischen der Sozialsphäre, der Privatsphäre und der Intimsphäre zu unterscheiden.
Bei Eingriffen in die Intimsphäre überwiegt das allgemeine Persönlichkeitsrecht immer, weil diese den unantastbaren Kernbereich des Persönlichkeitsschutzes darstellt.

Bei Personen des öffentlichen Lebens gelten im Grundsatz dieselben Maßstäbe, jedoch ist das gesteigerte Informationsbedürfnis und -interesse der Öffentlichkeit zu berücksichtigen. So kann die Berichterstattung über Gegenstände der Privatsphäre eines Politikers oder Prominenten unter Umständen eher zulässig sein, als bei einer Privatperson.
Die Intensität der Beeinträchtigung des Persönlichkeitsrechts erhöht sich durch die über das Internet verbreiteten Presseprodukte. Ein Presseprodukt, das im Internet in Persönlichkeitsrechte eingreift, ist im Vergleich zu ähnlichen Eingriffen in anderen Medien sehr lange und dauerhaft verfügbar und kann schnell und weit verbreitet werden. Wegen des für den mittlerweile weit überwiegenden Teil der Bevölkerung niedrigschwelligen Zugangs zum Internet kann außerdem leicht ein sehr großer Personenkreis erreicht werden. Dies erhöht regelmäßig die Gewichtung des Persönlichkeitsrechts in der Abwägung mit der Pressefreiheit.

2. Verdachtsberichterstattung

Ein über die allgemeine Abwägung hinaus besonders sensibler Bereich der Berichterstattung ist die sog. Verdachtsberichterstattung. Solange ein mutmaßlicher Täter noch nicht durch ein Gericht rechtskräftig verurteilt wurde, gilt zu seinen Gunsten zunächst die Unschuldsvermutung. Die Presse hat jedoch wiederum die verfassungsrechtlich gewährleistete Aufgabe, an der öffentlichen Meinungsbildung mitzuwirken sowie aktuelle Berichterstattung zu wichtigen Ereignissen der Zeitgeschichte vorzunehmen. Um diese Aufgaben sachgemäß erfüllen zu können, ist daher allgemein anerkannt, dass durch die Presse auch Mitteilungen bezüglich des Verdachts von Straftaten, die sog. Verdachtsberichterstattung, erfolgen können. Hierbei hat die Presse jedoch äußerst sensibel und vorsichtig vorzugehen, da von ihr ein signifikantes Maß an Beeinträchtigung („Prangerwirkung“) für den Betroffenen ausgehen kann. Bei Berichten über den Verdacht von Straftaten gilt daher, dass es zu einer besonders sorgfältigen Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen und dem Informationsinteresse der Öffentlichkeit kommen muss.

Beispielhaft kann in diesem Zusammenhang eine Berichterstattung genannt werden, der eine gerichtliche Auseinandersetzungen über ihre Zulässigkeit folgte:[6] Im Falle eines Kronzeugen in der Wirecard-Affäre wurde in einem Videobeitrag und einem nahezu wortgleichen Schriftbeitrag (Bild) neben dem Ermittlungsbeginn durch den Erlass eines Untersuchungshaftbefehls der Staatsanwaltschaft ebenfalls der volle Name des Tatverdächtigen genannt. Ebenso wurden jedoch auch Formulierungen wie „Schlüsselfigur“ oder „Strippenzieher“ in Verbindung mit schweren, angeblich durch den Tatverdächtigen begangenen Straftaten genannt. Außerdem enthielten die Beiträge Bildnisse des Kronzeugen, deren Verwendung er nicht zugestimmt hatte. Das Gericht stellte hierzu fest, dass durch den Erlass eines

6 LG München I, Urt. v. 20.04.2022 - 9 O 11679/20.

Untersuchungshaftbefehls zwar ein dringender Tatverdacht deutlich werde, dies jedoch keinesfalls mit der Erhebung einer Anklage zu vergleichen sei. Zu diesem Zeitpunkt müsse die Presse daher besonders sorgfältig vorgehen, da in der Öffentlichkeit allein die Einleitung eines Ermittlungsverfahrens bereits erheblich zur öffentlichen Meinungsbildung beitrage. Soweit die Berichterstattung darüber hinaus durch die Verwendung bestimmter Begrifflichkeiten oder Formulierungen den Eindruck erwecke, es handle sich bei der tatverdächtigen Person um einen (Haupt)täter, begründe dies eine nicht zulässige Verletzung der Unschuldsvermutung. Denn durch eine solche Schilderung werde außer Acht gelassen, dass sich das Verfahren lediglich im Ermittlungsverfahren befinde – vielmehr käme es hierdurch bereits zu einer medialen Vorverurteilung.[7]

3. Identifizierende Berichterstattung

Ebenfalls im Zusammenhang mit Verdachtsberichterstattung, aber auch mit anderen Gegenständen von Presseberichten relevant ist die Frage, ob die konkrete Identifikation des Protagonisten der Berichterstattung zulässig ist.
So wehrte sich beispielsweise ein Zahnarzt aus Köln gegen einen Artikel in welchem eine ihn betreffende Anklage thematisiert wurde.[8] Dabei wurde durch die publizierende Zeitung (bild.de) ebenfalls sein vollständiger Vorname, sein abgekürzter richtiger Nachname, sein Alter sowie die Lage seiner Praxis in der Kölner Innenstadt genannt.

Bei Berichten über den Verdacht von Straftaten, die eine Identifikation des Tatverdächtigen zulassen, gelten zunächst die Ausführungen bezüglich der Verdachtsberichterstattung gleichermaßen, sodass es einer besonders sorgfältigen Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen und dem Informationsinteresse der Öffentlichkeit bedarf. Eine identifizierende Berichterstattung ist auch nicht immer bereits dann unzulässig, wenn die Berichterstattung auch ohne Namensnennung erfolgen könnte – dann wäre nahezu jede identifizierende Berichterstattung unzulässig. Dies würde aber sowohl die Pressefreiheit als auch das Recht zur freien Meinungsäußerung von vornherein in unzulässiger Weise einschränken. Vielmehr ist im jeweiligen Einzelfall zu fragen, ob über das berechtigte Interesse an dem den Gegenstand der Berichterstattung bildenden Geschehen hinaus unter Berücksichtigung des Geheimhaltungsinteresses des Betroffenen auch – und wenn ja in welchem Umfang – ein berechtigtes Interesse der Öffentlichkeit an der konkreten handelnden Person besteht.[9]

Im Fall des Kölner Zahnarztes urteilte das Gericht, dass zunächst ein Berichterstattungsinteresse der Öffentlichkeit bestehe, da es sich um ein besonderes Verfahren handle. Der Zahnarzt habe eine gesellschaftlich hervorgehobene Stellung inne, was ebenfalls zur Rechtfertigung der Berichterstattung beitrage.[10]

Auch die Identifizierungsmöglichkeit für einen „beschränkten Kreis“ durch die erfolgte Berichterstattung sei noch in den Grenzen der Zulässigkeit, wobei jedoch offenbleibt, wann dieser beschränkte Kreis verlassen wird.
Im Falle einer öffentlichen Gerichtsverhandlung liege außerdem keine Verdachtsberichterstattung mehr vor. Es handelt sich um eine Berichterstattung über ein öffentliches Ereignis, das tatsächlich so stattgefunden hat. Eine grds. erforderliche Möglichkeit zur Stellungnahme ist daher bei Angeklagten nun nicht erforderlich. Dies würde eine aktuelle Gerichtsberichterstattung erheblich einschränken. Die Abwägung zwischen dem Informationsinteresse der Öffentlichkeit und dem Persönlichkeitsrecht des Angeklagten verlief hier daher zugunsten des Informationsinteresses.

Zuletzt konkretisierte der Bundesgerichtshof (BGH) in einem aktuellen Urteil erneut die Anforderungen an die identifizierende Verdachtsberichterstattung:
In dem zugrundeliegenden Fall wurde einem ehemaligen armenischen Botschafter vorgeworfen, ein „Dieb im Gesetz“ zu sein. Die Richter in Karlsruhe statuierten, dass für eine identifizierende Verdachtsberichterstattung jedenfalls ein Mindestbestand an Beweistatsachen, die für den Wahrheitsgehalt der Information sprechen und ihr damit erst „Öffentlichkeitswert“ verleihen,

7 https://www.lto.de/recht/nachrichten/n/lg-muenchen-i-901167920-bild-zeitung-bericht-artikel-namensnennung-foto-wirecard-kronzeuge-oliver-b-vorverurteilung-unschuldsvermutung /(zuletzt abgerufen am 31.10.2023).

8 LG Köln, Urt. v. 31.05.2022 - VI ZR 95/21.

9 OLG Dresden, Urt. v. 29.3.2022 – 4 U 178/22.

10 https://www.lto.de/recht/hintergruende/h/bgh-vizr9521-medien-berichterstattung-gericht-strafverfahren-identifikation-persoenlichkeitsrecht /(zuletzt abgerufen am 31.10.2023).

erforderlich sei. Die Darstellung darf ferner keine Vorverurteilung des Betroffenen enthalten; sie darf also nicht durch eine präjudizierende Darstellung den unzutreffenden Eindruck erwecken, der Betroffene sei der ihm vorgeworfenen Handlung bereits überführt. Auch ist vor der Veröffentlichung regelmäßig eine Stellungnahme des Betroffenen einzuholen. Schließlich muss es sich um einen Vorgang von gravierendem Gewicht handeln, dessen Mitteilung durch ein Informationsbedürfnis der Allgemeinheit gerechtfertigt ist.

4. Clickbaiting

Zuletzt nimmt im digitalen Bereich die Nutzung von besonderen Methoden durch die Medienschaffenden zu, um mehr Clicks zu generieren und die Aufmerksamkeit der Nutzer:innen für die eigenen Inhalte zu gewinnen. Bei einem prominenten Fall des sog. „Clickbaitings", wurde ein Bild des Moderators Günter Jauch ohne dessen Einwilligung für die Bewerbung bzw. Aufmachung eines verlinkten Artikels verwendet, wobei der Beitrag in keinem Bezug zu seiner Person stand, sich also gänzlich anderen Inhalten widmete.
Der BGH wies die Medien hier in ihre Schranken und stärkte das allgemeine Persönlichkeitsrecht des Betroffenen:[11] Es sei nicht zulässig das Bild einer Person des öffentlichen Lebens zu nutzen, wenn in dem verlinkten Artikel keinerlei Bezug zu dieser Person hergestellt wird. Mittelbar werden hierdurch auch die Adressaten der Berichterstattung vor Irreführung durch das Erwecken des Interesses mit prominenten Gesichtern geschützt.

IV. Bedeutung für Hochschulen und Forschungseinrichtungen

Die Freiheit der Presse ist als Grundpfeiler unserer Demokratie für jeden Einzelnen relevant. Zum einen können auch Hochschulen und Forschungseinrichtungen sowie ihre Mitarbeiter:innen Gegenstand von medialer Berichterstattung werden. Zum anderen ist die Aufrechterhaltung der Medienvielfalt und der Schutz von Medienschaffenden auch im Interesse der Bildung und Entwicklung der Gesellschaft hierzulande. Daher sind die Reaktionen und Ansätze der Gesetzgeber grundsätzlich zu begrüßen und es bleibt abzuwarten, ob den Gefahren und Risiken für die Pressefreiheit hiermit Abhilfe geschaffen werden kann.

11 BGH Urt. v. 12.01.2021 - I ZR 120/19.

Unterm Christbaum liegt ’ne Handreichung

Datenschutzaufsichtsbehörden veröffentlichen Handreichung zur Nutzung von Microsoft 365

Von Klaus Palenberg

Bereits im November 2022 hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Einschätzung zur Nutzung von Microsoft 365 abgegeben. Dabei kam sie zu dem Ergebnis, dass die von Microsoft vorgegebene Standard-Auftragsverarbeitungsvereinbarung (Data Protection Addendum – DPA) nicht mit der Datenschutzgrundverordnung (DSGVO) vereinbar ist. Nachdem Änderungsgespräche mit Microsoft gescheitert sind, hat nun eine Arbeitsgruppe der DSK (AG DSK „Microsoft-Onlinedienste“), bestehend aus mehreren Landesdatenschutzaufsichtsbehörden[1], eine Handreichung[2] zum Abschluss einer Auftragsverarbeitungsvereinbarung für den Einsatz von Microsoft 365 herausgegeben. Diese Handreichung richtet sich an Verantwortliche, also die Nutzenden der Software und nicht an Microsoft selbst.

I. Ja ist denn heut‘ scho‘ Weihnachten?

Es mutet wie ein großes Geschenk der DSK an, nachdem sie im November 2022 den Einsatz von Microsoft 365 für schwerlich vereinbar mit der DSGVO erklärt hatte. Daraufhin gab es zum Teil scharfe Kritik an den Datenschutzaufsichtsbehörden.[3] Ein den Kritikern besonders unter den Nägeln brennender Punkt ist, dass die Datenschutzaufsichtsbehörden bislang stets erklärt hatten, was datenschutzrechtlich nicht möglich sei. Wie aber in der Praxis gerade seit Corona vielgenutzte Software datenschutzkonform einsetzbar ist, dazu schwiegen sie sich laut aus. Nun scheinen die Datenschutzaufsichtsbehörden die Rufe erhört zu haben und den Kritikern ihre Wünsche nach einer Empfehlung, wie Microsoft 365 datenschutzkonform genutzt werden kann, erfüllt zu haben. Doch wie es manchmal ist, ist am Ende bei einigen Geschenken die Verpackung das Schönste daran. Ob dies bei dieser Handreichung ebenfalls der Fall und die Freude bei den Verantwortlichen ebenso groß wie über ein Paar Socken unterm Weihnachtsbaum ist, soll dieser Beitrag klären.

II. Die Vorbemerkung zur Handreichung

Den inhaltlichen Hinweisen und Empfehlungen werden in der Handreichung zunächst einige Vorbemerkungen vorangeschickt. Dabei wird als erstes der Hintergrund der Handreichung dargelegt. Beim Einsatz von Produkten wie Microsoft 365 werden Daten, in diesem Fall an Microsoft, übermittelt. Betreffen diese Daten auch personenbezogene Merkmale, sind die nutzenden öffentlichen und nicht-öffentlichen Stellen Verantwortliche

1 Unter ihnen befinden sich der Bayerische Landesbeauftragte für den Datenschutz, der Landesbeauftragte für den Datenschutz Niedersachsen und die Landesbeauftragte für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen.

2 Abrufbar unter https://www.ldi.nrw.de/datei/handreichung-fuer-die-verantwortlichen-zum-abschluss-einer-auftragsverarbeitungsvereinbarung (zuletzt abgerufen am 15.11.2023).

3 Siehe beispielsweise https://www.heise.de/news/Datenschutzbehoerden-erklaeren-den-Einsatz-von-Microsoft-365-fuer-rechtswidrig-4931745.html (zuletzt abgerufen am 15.11.2023).

i.S.d. DSGVO und Microsoft Auftragsverarbeiter i.S.d. DSGVO.[4] Die Grundlage für die Datenübermittlung an Microsoft hat in diesem Fall eine Auftragsverarbeitungsvereinbarung zu bilden. Im Falle von Microsoft 365 bietet Microsoft seinen Kunden eine Standard-Auftragsverarbeitungsvereinbarung[5] an. Diese Vereinbarung hält die DSK aber nach Feststellungen im November 2022 für nicht datenschutzkonform, da die Anforderungen nach Art. 28 Abs. 3 DSGVO nicht erfüllt seien. Den größten Missstand sah sie in der mangelnden Transparenz in Hinblick auf die Verarbeitung der übermittelten personenbezogenen Daten für eigene Zwecke und deren Rechtmäßigkeit.

Als Verantwortliche i.S.d. DSGVO sind aber die öffentlichen und nicht-öffentlichen Stellen nach Art. 5 Abs. 2 DSGVO für die datenschutzkonforme Verarbeitung der Daten entsprechend rechenschaftspflichtig. Dies umfasst nach Art. 28 Abs. 1 DSGVO auch die Auswahl von Auftragsverarbeitern, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.[6] Da aber die von Microsoft angebotene Standard-Auftragsverarbeitungsvereinbarung eine rechtmäßige Auftragsverarbeitung nicht garantieren kann, schlussfolgert die Arbeitsgruppe aus Art. 28 DSGVO, dass die Verantwortlichen eine angepasste Auftragsverarbeitungsvereinbarung mit Microsoft abzuschließen haben.

Darin besteht jedoch die Krux der gesamten Handreichung, was die Arbeitsgruppe auch offen zugibt. Denn zurecht weist sie daraufhin, dass „Änderungen oder Ergänzungen der Vertragsbedingungen mit Microsoft […] nicht alleine in der Hand der einsetzenden öffentlichen und nicht-öffentlichen Stellen [liegen], sondern […] davon abhängig [sind], dass Microsoft als Vertragspartner diesen zustimmt".[7] Nach den, auch von den Datenschutzaufsichtsbehörden, bislang in der Zusammenarbeit mit Microsoft gemachten Erfahrungen bestehen jedoch einige Zweifel an der Bereitschaft von Microsoft, diese Zustimmung zu erteilen.

Zusätzlich zu diesen Vertragsanpassungen könnten die Verantwortlichen auch eigene technische und organisatorische Maßnahmen, wie die Verwendung pseudonymer Mailadressen für die Beschäftigten, ergreifen.[8] Oberste Priorität habe aber das Hinwirken auf eine Auftragsverarbeitungsvereinbarung, die die Anforderungen nach Art. 28 Abs. 3 DSGVO erfülle.

Um dies zu unterstützen, enthält die Handreichung verschiedene Hinweise, die sich an den Mängeln orientieren, die die DSK an der Standard-Auftragsverarbeitungsvereinbarung von Microsoft kritisiert hatte. Aufgebaut sind diese Hinweise in einem Kurzüberblick (auf immer noch fünf Seiten) zu Beginn in Abschnitt II und einer Langversion in einer Anlage, die auch die datenschutzrechtlichen Erwägungen der Arbeitsgruppe für die gemachten Vorschläge und Hinweise enthält.

Kurz vor dem Ende der Vorbemerkungen folgt eine Einschränkung der Reichweite der Handreichung. Denn ausdrücklich ausgenommen ist ein weiteres äußerst praxisrelevantes Problem: die Übermittlung personenbezogener Daten in Drittländer wie die USA. Dies ist zwar nachvollziehbar, da der Angemessenheitsbeschluss zum EU-U.S. Data Privacy Framework[9] noch recht jung und das Thema hochumstritten ist. Allerdings wären aktuelle

---

4 Zu den Voraussetzungen und Folgen einer gemeinsamen Verantwortlichkeit siehe Baur, Auch aus kleiner Kraft folgt große Verantwortung, DFN-Infobrief 08/2018.

5 Nicht zu verwechseln mit den Standardvertragsklauseln der Kommission; hierzu John, New Schrems, new Me(crosoft), DFN-Infobrief Recht 02/2022.

6 Zu den weiteren Voraussetzungen und Anforderungen an eine Auftragsverarbeitung nach Art. 28 DSGVO siehe Mörike, Im Auftrag des Verantwortlichen, DFN-Infobrief Recht 04/2019.

7 Handreichung für die Verantwortlichen zum Abschluss einer Auftragsverarbeitungsvereinbarung gem. Art. 28 Abs. 3 DSGVO mit Microsoft für den Einsatz von „Microsoft 365", S. 2.

8 Allgemein zu den erforderlichen Maßnahmen datenverarbeitender Stellen nach der DSGVO siehe Sydow, Neues Datenschutzrecht = neue Sicherheit für Daten?, DFN Infobrief Recht 09/2016.

9 Hierzu John, Das neue Data Privacy Shamework?, DFN-Infobrief Recht 10/2023; Tech, Kurzbeitrag: Data Privacy Framework – Die nächste Vollschremsung?, DFN-Infobrief Recht 05/2023; Palenberg, Auf die Schremse treten?, DFN-Infobrief Recht 02/2023; Mc Grath, Ausgeschremst?, DFN-Infobrief Recht 05/2022.

hilfreiche Ausführungen einer Datenschutzaufsichtsbehörde zu diesem Problemkreis[10] wie Schnee am Heiligen Abend. Auch geht die Arbeitsgruppe nicht auf technische Unterschiede ein, die sich aufgrund verschiedener Versionen und Funktionsweisen von Microsoft 365 ergeben können.

Abschließend betont die Arbeitsgruppe, dass die abzuschließenden Zusatzvereinbarungen klarstellen sollten, dass sie anderen Nutzungsbedingungen oder Auftragsverarbeitungsvereinbarungen, wie dem DPA, vorgingen und im Kollisionsfalle anzuwenden sind.

III. Die wesentlichen Handlungshinweise

Die wesentlichen Handlungshinweise in Abschnitt II und der Anlage gliedern sich in sieben Unterpunkte. Dabei beinhalten die gegebenen Hinweise in erster Linie eine Aufzählung der Pflichten der Verantwortlichen bzw. die vorgeschriebenen Anforderungen an eine Auftragsverarbeitungsvereinbarung nach Art. 28 Abs. 3 DSGVO. Diese gesetzlichen Anordnungen werden mit den Regelungen des DPA in Relation gesetzt und bewertet. Hieraus leitet die Handreichung dann die wesentlichen Änderungspunkte des DPA ab.

1. Festlegung von Art und Zweck der Verarbeitung, Art der personenbezogenen Daten

Nach Art. 28 Abs. 3 S. 1 DSGVO muss eine Auftragsverarbeitungsvereinbarung u.a. Art und Zweck der Verarbeitung enthalten. Dabei kann der Verantwortliche lediglich die Verarbeitungszwecke beauftragen, für die er sich selbst auf eine Rechtsgrundlage stützen kann. Das DPA enthält aber auch Ausführungen zu Zwecken, die allein im Interesse von Microsoft liegen, wie etwa die Produktverbesserung, für die in der Regel keine Grundlage auf Seiten der Verantwortlichen besteht. Solche Zwecke sollten von der Auftragsverarbeitungsvereinbarung ausgenommen werden. Auch die Art der personenbezogenen Daten muss sich zumindest kategorisiert unmittelbar aus der Auftragsverarbeitungsvereinbarung ergeben. Dies kann durch Verweis auf das Verzeichnis der Verarbeitungstätigkeiten oder auf andere Weise, wie etwa einer tabellarischen Aufstellung erfolgen.

2. Eigene Verantwortlichkeit Microsofts im Rahmen der Verarbeitung für Geschäftstätigkeiten, die durch Bereitstellung der Produkte und Services an den Kunden veranlasst sind

Sollte sich eine Verarbeitung personenbezogener Daten durch Microsoft zu eigenen Zwecken nicht pauschal ausschließen lassen, haben die Verantwortlichen zunächst zu klären, ob und falls ja, welche Rechtsgrundlage für eine Datenweitergabe an Microsoft besteht. Dies ist angesichts der an wesentlichen Stellen unklaren Formulierungen des DPA aber nicht ohne Weiteres möglich. Zur Feststellung einer Rechtsgrundlage ist es deshalb erforderlich, zu klären, welche Kategorien personenbezogener Daten für welche eigenen Geschäftszwecke von Microsoft genutzt werden sollen.

In Hinblick auf Telemetrie- und Diagnosedaten gilt es zudem zuerst zu klären, wie sie von Microsoft verarbeitet werden, da hiervon abhängig ist, ob es sich überhaupt um personenbeziehbare Daten handelt und das DPA anwendbar ist. Dabei sind auch arbeitsrechtliche Implikationen, wie eine Beteiligung der Personalvertretung, zu bedenken.

Gerade bei der Nutzung von Microsoft 365 durch öffentliche Stellen bestehen besonders hohe Anforderungen an die Rechtmäßigkeit einer Verarbeitung personenbezogener Daten durch Microsoft zu eigenen Zwecken. So kann etwa Art. 6 Abs. 1 S. 1 Buchst. f DSGVO als Rechtsgrundlage der Verarbeitung durch spezielleres Fachrecht ausgeschlossen sein.

3. Weisungsbindung, Offenlegung verarbeiteter Daten, Erfüllung rechtlicher Verpflichtungen

Nach Einschätzung der Arbeitsgruppe sind die Regelungen zur Weisungsbindung gemäß Art. 29 DSGVO des DPAs widersprüchlich. Gerade deshalb sollte das Bestehen eines einseitigen Weisungsrechts des Verantwortlichen klargestellt werden.

Das DPA sieht die Möglichkeit einer Offenlegung von personenbezogenen Daten an Institutionen innerhalb der EU vor, aber auch gegenüber Institutionen in unsicheren Drittländern

10 Zu diesem speziell in Hinblick auf Microsoft 365 siehe Tiessen, Alles in der Schwebe, DFN-Infobrief Recht, 04/2021.

falls dort entsprechende rechtliche Verpflichtungen bestehen. Diese Verpflichtung ist jedoch nicht mit den Vorgaben der DSGVO vereinbar und muss nach Einschätzung der Arbeitsgruppe vertraglich abbedungen werden.

4. Umsetzung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO

Gemäß Art. 32 DSGVO haben der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Schutzniveau für die Rechte und Freiheiten natürlicher Personen zu gewährleisten.

Diesbezüglich räumt das DPA Microsoft nach Ansicht der Arbeitsgruppe einen zu großen Spielraum ein, welche Maßnahmen ergriffen werden können. Auf der einen Seite bleibt offen, welche Daten Microsoft zusätzlich zu den Nutzerdaten zu diesem Zweck verarbeitet und wie umfangreich die Verarbeitung dann erfolgt. Auf der anderen Seite bleibt das DPA aber auch hinter den Erwartungen der Arbeitsgruppe zurück und lässt wichtige Instrumente zum Schutz besonders sensibler Daten i.S.d. Art. 9 DSGVO (Art. 9-Daten) unerwähnt.

Hier fordert die Arbeitsgruppe zum einen eine Beschränkung auf die tatsächlich erforderlichen Kategorien an Daten und das notwendige Maß der Verarbeitung dieser, aber zum anderen die Ergänzung der notwendigen Maßnahmen zum Schutz der Art. 9-Daten.

5. Löschen personenbezogener Daten

Zwar enthält das DPA einen mehrstufigen Löschprozess mit abgestuften Löschfristen. Diese sind der Arbeitsgruppe aber teilweise zu lang. Auch sind bestimmte Datensätze ausgenommen und müssten vertraglich miteinzogen werden.

6. Information über Unterauftragsverarbeiter

Für den Fall, dass sich Microsoft wiederum selbst weiterer Auftragsverarbeiter bedient, sind diese Unterauftragsverarbeiter i.S.d. Art. 28 Abs. 2, 4 DSGVO. In diesem Fall sieht Art. 28 Abs. 2 S. 2 DSGVO eine Informationspflicht des Auftragsverarbeiters an den Verantwortlichen vor. Das DPA statuiert diesbezüglich aber nach Ansicht der Arbeitsgruppe eine „Holschuld“ des Verantwortlichen. Dementsprechend sollte klargestellt werden, dass nicht der Verantwortliche nachfragen oder sich informieren muss, sondern Microsoft proaktiv über eine Unterauftragsverarbeitung informieren muss. Diese Information sollte auch detaillierte Angaben wie Namen oder Anschrift des Unterauftragsverarbeiters oder eine Kontaktperson bei diesem beinhalten.

7. Weitere Hinweise

Abschließend führt die Handreichung noch weitere Hinweise auf. So wird der Betrieb von Microsoft auf eigenen IT-Strukturen („On-Premises-Lösung“) nahegelegt, um beispielsweise eine Übermittlung der Daten an Microsoft steuern oder unterbinden zu können.

Von einer Nutzung privater Microsoft-Accounts oder privater Hardware („Bring your own device“ – BYOD) rät die Arbeitsgruppe gänzlich ab.
In Hinblick auf eine Nutzung von Microsoft 365 in Bildungseinrichtungen erinnert die Arbeitsgruppe an die Schwierigkeiten, eine wirksame Einwilligung in die Datenverarbeitung der Schülerinnen und Schüler bzw. ihrer Eltern einzuholen.[11]

IV. Bedeutung der Handreichung für Hochschulen und Forschungseinrichtungen

Die Handreichung enthält eine Vielzahl an richtigen und wichtigen Anmerkungen zum DPA. Sämtliche Vorschläge und Änderungshinweise zur Rechtmäßigkeit der Auftragsverarbeitung sind entweder notwendig oder zumindest wünschenswert. Alles hängt aber am Ende von Microsoft ab.
Sollten sich Verantwortliche die Mühe machen und die Handreichung umsetzen, liegt es an Microsoft, diesen Änderungsvertrag

11 Zur Problematik hinsichtlich der Lehrpersonen siehe John, Kurzbeitrag: Alles neu macht der EuGH, DFN-Infobrief Recht 06/2023; John, Die Beschäftigung mit Beschäftigtendaten, DFN-Infobrief Recht 10/2022.

auch anzunehmen. Sollte Microsoft dies, wie zu befürchten ist, ablehnen, würde Microsoft in Bezug auf die Handreichung aus Sicht der Verantwortlichen leider den Grinch[12] mimen.

Rein rechtlich betrachtet, bliebe es dann bei den Regelungen des DPA und damit, zumindest nach Ansicht der DSK, bei der Rechtswidrigkeit der Auftragsverarbeitung durch Microsoft. Eine Nutzung von Produkten der Microsoft 365-Gruppe stünde dann unter dem Damoklesschwert des Einschreitens der Datenschutzaufsichtsbehörden. Rein praktisch gesehen ist dies wenig befriedigend, denn wirkliche Alternativen bietet der Markt aktuell nicht. Damit lässt sich vielleicht auch die bisherige hartnäckige Weigerung von Microsoft erklären, auf die Forderungen der DSK einzugehen. Inwieweit ein gemeinsames Auftreten, beispielsweise eines Zusammenschlusses von Hochschulen daran etwas ändern könnte, bleibt ungewiss, wäre aber unter Umständen einen Versuch wert. Sollte die durch diesen Zusammenschluss zustandekommende große Anzahl an potenziellen Nutzenden und die damit verbundenen Einnahmen Microsoft schließlich doch beeindrucken und zur Umsetzung der mit der Handreichung geforderten Änderungen bewegen, wäre die Handreichung am Ende doch das versprochene Geschenk.

12 Der Grinch ist ein Fabelwesen aus einem US-amerikanischen Kinderbuch, das Weihnachten hasst und deshalb alle Geschenke stiehlt (https://de.wikipedia.org/wiki/Wie_der_Grinch_Weihnachten_gestohlen_hat).

Kurzbeitrag: Leise rieselt der Score

Die Schufa beginnt mit der Löschung der Daten von 20 Millionen Handybesitzern

von Marc-Philipp Geiselmann

Die Schufa Holding AG, auch bekannt als „Schutzgemeinschaft für allgemeine Kreditsicherung", ist eines der einflussreichsten Unternehmen Deutschlands. Sie präsentiert sich selbst in einem positiven Licht und betont, dass ihre Produkte das Vertrauen zwischen Geschäftspartnern fördern würden, auch wenn diese sich nicht persönlich kennen. Allerdings ist auch klar, dass bei einem negativen Score Misstrauen geschürt wird und potentielle Geschäftspartner aufgrund dessen „den Daumen senken". Der Score der Schufa kann für Verbraucher sowohl positiv als auch negativ ausfallen. Daher ist es von großem Interesse, welche Daten bei der Berechnung dieses Scores berücksichtigt werden. Die Transparenz der Schufa bei der Datenauswahl ist ein wichtiges Thema, das die Öffentlichkeit betrifft.

I. Einstieg

Die Schufa sammelte Positivdaten, die von Telekommunikationsanbietern übermittelt wurden. Darunter fallen beispielsweise Art und Dauer des abgeschlossenen Mobilfunkvertrags.

Die Datenschutzkonferenz des Bundes und der Länder (DSK) kam bereits am 11. Juni 2018 zu dem Ergebnis, dass für die Übermittlung und Verarbeitung dieser Daten kein überwiegendes „berechtigtes Interesse" gemäß Art. 6 Abs. 1 lit. f DSGVO besteht und es daher einer Einwilligung der betroffenen Personen bedarf. Diese hatten die Telekommunikationsanbieter jedoch nicht eingeholt, sondern lediglich in ihren Allgemeinen Geschäftsbedingungen auf die Übermittlung an Auskunfteien hingewiesen. Die DSK erhielt ihre Einschätzung am 22. September 2021 durch einen erneuten Beschluss aufrecht.[1] Aufgrund dessen wurde die Weitergabe der Daten durch die Telekommunikationsanbieter Anfang 2022 gestoppt. Die bereits übermittelten Daten blieben jedoch bei der Schufa gespeichert. Zumindest vorübergehend …

II. Entscheidung der Schufa

In einer überraschenden Entscheidung gab die Schufa am 19. Oktober 2023 bekannt, die Daten von 20 Millionen Handybesitzern aus ihrer Datenbank ab dem 20. Oktober 2023 zu löschen.[2] Dadurch sollen die Privatsphäre und die digitalen Rechte der Verbraucher gestärkt werden.

Bis Anfang 2022 hatte die Schufa nach eigenen Angaben die Vertragsdaten von Kunden der Telekommunikationsanbieter zur Prävention von Betrug gesammelt. Die Schufa nutzte diese gesammelten Daten jedoch auch zur Berechnung des Bank-Scores zur Beurteilung der Kreditwürdigkeit. Verbraucherschützer kritisieren seit Jahren, dass die Verwendung dieser Daten für die Score-Berechnung irrelevant ist. Die Datenschutzkonferenz der Länder hat festgestellt, dass für die Übermittlung von Positivdaten durch Telekommunikationsanbieter zwar ein berechtigtes Interesse an der Verbesserung der Qualität der Bonitätsbewertung und am Schutz vor Kreditrisiken besteht. Besondere Umstände und Interessen der Verantwortlichen an der Verarbeitung bestimmter Positivdaten, die die Interessen, Grundrechte und Grundfreiheiten der Betroffenen überwiegen,

1 https://www.datenschutzkonferenz-online.de/media/dskb/20210929_top_07_beschluss_positivdaten.pdf (zuletzt abgerufen am 14.11.2023).

2 https://www.schufa.de/themenportal/schufa-loescht-telkodaten/ (zuletzt abgerufen am 14.11.2023).

konnte die DSK im Rahmen ihrer Prüfung jedoch nicht feststellen. Die Kunden hätten also in die Weitergabe und Verarbeitung durch die Schufa einwilligen müssen.

Nach Angaben der Schufa erfolgt die Löschung der Daten in Übereinstimmung mit dem Beschluss der Datenschutzkonferenz der Länder.

Allerdings ist der Druck auf die Telekommunikationsanbieter nach dem Urteil des Landgerichts München I vom 25. April 2023, wonach die Datenübermittlung an die Schufa nicht ohne Einwilligung hätte erfolgen dürfen, offenbar zu groß geworden.[3] Anfang Oktober kündigten zwei Kölner Anwaltskanzleien an, tausende Klagen gegen die Telekommunikationsanbieter zu erheben. Für die Kläger steht ein Schadensersatz in Höhe von jeweils bis zu 5.000 Euro zuzüglich der Kosten für die Rechtsverfolgung im Raum. Die Schufa kommt nun durch die Löschung der Daten vielen Prozessen zuvor. Für eine mögliche Klage gegen den Telekommunikationsanbieter benötigen die Kunden eine Datenkopie der Schufa, um zu überprüfen, ob ihre Daten weitergegeben wurden.

Ob diese Information für den Verbraucher positiv oder negativ ist, hängt von der individuellen Situation ab. Die Schufa gibt selbst an, dass der Score bei 53 Prozent der betroffenen Personen nun niedriger und somit schlechter ausfallen wird, während er bei 47 Prozent höher liegen wird. Dies liegt daran, dass sich eine geringe Anzahl von Verträgen mit langen Laufzeiten positiv auf den Score auswirkt. Die Änderungen beim Score werden nicht groß ausfallen, die Schufa spricht lediglich von „marginalen“ Veränderungen.

III. Hochschulbezug

Für Hochschulen ist es im Falle einer Datenweitergabe an Dritte von Bedeutung, die zugrundeliegende Rechtsgrundlage zu kennen. Regelmäßige Datenweitergaben können ein erhebliches finanzielles Risiko darstellen, da ein Schadensersatzanspruch von bis zu 5.000 Euro pro Fall besteht. Es ist ratsam, dieses Risiko zu vermeiden.

Auch Hochschulen und Beschäftigte von Hochschulen könnten von einer Datenübermittlung betroffen sein.

Ebenso für Studenten spielt die Kreditwürdigkeit eine wichtige Rolle, insbesondere, wenn sie einen Studienkredit beantragen möchten.

3 https://www.verbraucherzentrale.nrw/sites/default/files/2023-05/2023-04-25_lg-munchen-i_urteil_geschw.pdf (zuletzt abgerufen am 14.11.2023); Das Urteil war bei Fertigstellung des Beitrags noch nicht rechtskräftig.

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