infobrief recht DFN

6 / 2022
Juni 2022

Data Act: Mehr Daten für alle – check!
Der Entwurf der Europäischen Kommission zur Neugestaltung des Datenaustauschs

Geheim bis das Erbe uns scheidet
Der neue § 4 TTDSG und seine Auswirkungen auf den digitalen Nachlass

Brüssel reguliert das schon
EU-Institutionen einigen sich final auf DMA und DSA

Kurzbeitrag: Künast die Dritte
Die Entscheidung des Landgerichts Frankfurt am Main zur Sperrpflicht von Meta

Data Act: Mehr Daten für alle – check!

Der Entwurf der Europäischen Kommission zur Neugestaltung des Datenaustauschs

von Johanna Schaller

Während das Thema Datenschutz aktuell in aller Munde ist, stellen Daten auf der anderen Seite das Herzstück der digitalen Wirtschaft dar. Unternehmen verfolgen daher zunehmend die Bestrebung, den Wert der Daten möglichst umfassend und effizient zu nutzen. Der Data Act nimmt eine sektorübergreifende Neugestaltung der Datennutzung und des Datenaustauschs vor und bietet so die Möglichkeit, das Wertschöpfungspotential von Daten erheblich zu verändern und zu verbessern.

I. Einleitung

Der „Data Act" ist ein Verordnungsentwurf für nicht-personenbezogene Daten, den die Europäische Kommission am 23. Februar 2022 vorgelegt hat. Die neuen Regeln sollen für Hersteller von vernetzten Produkten, Anbieter digitaler Dienste und Nutzer in der Europäischen Union (EU) gelten.

Der Entwurf definiert die Vorschläge der Kommission für den Zugang und die gemeinsame Nutzung von Daten, die Bedingungen für den Zugang durch öffentliche Einrichtungen, die internationale Datenübertragung, Cloud-Switching und Interoperabilität. „Die Menge der von Menschen und Maschinen erzeugten Daten nimmt exponentiell zu, aber die meisten Daten bleiben ungenutzt oder ihr Wert konzentriert sich in den Händen relativ weniger großer Unternehmen", heißt es in dem Vorschlag.

Die Kommission beabsichtigt das Potenzial der datengesteuerten Innovation durch den Data Act freizusetzen, indem sie rechtliche Verpflichtungen und Regelungen für die gemeinsame Nutzung von Daten schafft. Europäische Verordnungen entfalten, im Gegensatz zu Richtlinien, unmittelbare Geltung in den Mitgliedsstaaten. Eine Umsetzung durch nationale Gesetze ist daher nicht erforderlich. Jedoch können ggf. Änderungen und Anpassungen in den bestehenden Gesetzen notwendig sein, um den Vorgaben der Verordnung nicht im Wege zu stehen.

II. Recht auf Zugang

Der Data Act führt den Grundsatz ein, dass jeder Nutzer, ob Einzelperson oder Organisation, Zugang zu den Daten haben sollte, zu deren Erzeugung er beigetragen hat. Umgekehrt sollen vernetzte Produkte (connected products) und damit verbundene Dienste (related services), einschließlich virtueller Assistenten, die Daten dem Nutzer standardmäßig in zugänglicher Form zur Verfügung stellen. Der Nutzer kann mit den Daten frei verfahren, sie also auch an Dritte weitergeben. Überdies müssen dem Nutzer vor Abschluss eines Vertrages über den Kauf oder die Miete eines Produktes Mindestinformationen, wie Art und Umfang der voraussichtlich generierten Daten, geplante Verwendungszwecke und Angaben zum Dateninhaber, zur Verfügung gestellt werden.

Als „Nutzer" gelten insbesondere Leistungsempfänger, Eigentümer, Mieter oder Leasingnehmer eines Produkts. Der Entwurf enthält eine komplexe Definition der von dem Data Act erfassten „Produkte" und zielt dabei im Kern auf elektronische Geräte ab, die sozusagen beiläufig Umwelt- oder Nutzungsdaten erfassen und exportieren können. Geräte, die vorrangig zur Speicherung von Daten dienen oder menschlichen Input erfordern, um Inhalte und Daten zu generieren, sollen keine unter den Data Act fallenden Produkte darstellen.
Da viele smarte Internet of Things (IoT)-Geräte sowohl menschlichen Input benötigen als auch Daten beiläufig erfassen, birgt

diese Regelung derzeit noch eine erhebliche Rechtsunsicherheit.[1] Für den Begriff der datengenerierenden „Nutzung“ durch den Nutzer ist nach den Erwägungsgründen des Entwurfs ein weites Verständnis zugrunde zu legen. Es mangelt jedoch an hinreichender Klarheit, was im Einzelfall unter den Begriff fällt und welcher Zusammenhang zwischen Nutzung und Datum bestehen muss. Zudem ist zu klären, welchen konkreten Beitrag der Nutzer zur Generierung der Daten geleistet haben muss. Hierzu kann der Entwurf so verstanden werden, dass es allein auf die Nutzung des Produkts ankommt, nicht jedoch zwingend auf die Nutzung durch den Nutzer selbst.

Darüber hinaus kann der Nutzer auch vom Dateninhaber die Weitergabe der Daten an einen Dritten verlangen.
Der Dateninhaber muss die Daten dem Dritten sodann “unter fairen, vernünftigen und nicht-diskriminierenden Bedingungen, auf transparente Weise” zur Verfügung stellen, also mit dem Datenempfänger einen Datenlizenzvertrag abschließen. Der Dateninhaber unterliegt insofern einem Kontrahierungszwang unter den sog. FRAND-Bedingungen.[2] Der Dateninhaber darf von dem Datenempfänger für die Übermittlung der Daten eine angemessene Vergütung verlangen. Den Dateninhabern ist es nicht möglich, die Weitergabe der Daten durch den Nutzer technisch zu verhindern. Sie können nur Informationen anfordern, um zu überprüfen, ob die Anfrage von einem Nutzer oder einer autorisierten Partei stammt. Darüber hinaus verbietet der Entwurf exklusive Datenlizenzierungen, ausgenommen den Fall, dass der Nutzer in die Exklusivitätsvereinbarung eingewilligt hat.

Zu beachten ist, dass durch das Recht des Nutzers, seine Daten frei vom Dateninhaber zu erhalten und an Dritte weiterzugeben, eine Umgehung des Datenlizenzvertrages und der Vergütung möglich und denkbar ist.
Eine Einschränkung erfährt diese Gestaltungsmöglichkeit jedoch wiederum bei Geschäftsgeheimnissen: Hier kann der Dateninhaber dem Nutzer die freie Weitergabe verbieten oder Maßnahmen zur Wahrung der Vertraulichkeit der Daten und der Geschäftsgeheimnisse vereinbaren. Darüber hinaus hindert das Vorliegen von Geschäftsgeheimnissen das Recht des Nutzers auf Zugang zu den Daten jedoch nicht.

Die übermittelten Daten dürfen nicht dazu verwendet werden, Produkte zu entwickeln, die mit dem Dateninhaber konkurrieren. Nicht von diesem Verbot erfasst ist aber wohl die Entwicklung konkurrierender Leistungen. Auch ist noch unklar, welche Folgen ein Verstoß entfalten soll und in welchem Umfang das Konkurrenzverbot gilt – ob beispielsweise nur bei Vorsatz oder auch bei Vorliegen einfacher Fahrlässigkeit sowie wenn nicht wirtschaftliche, sondern allein wissenschaftliche Forschungszwecke im Vordergrund stehen.[3]

Untersagt ist es den Dateninhabern, Nutzern und Dritten nach dem Entwurf, die Daten an Organisationen weiterzugeben, die im Rahmen des Gesetzes über digitale Märkte (DMA) als sog. „Gatekeeper“ bezeichnet werden. Den Gatekeepern wiederum ist es untersagt, den Nutzer aufzufordern, Daten mit ihnen zu teilen oder Daten zu erhalten. Hiermit sollen große Konzerne, wie Google und Meta, in ihrer Datenmacht beschränkt werden.

Darüber hinaus sieht der Entwurf eine weitere entscheidende Regelung vor: Der Dateninhaber darf nicht-personenbezogene Daten, die durch die Nutzung eines Produkts oder eines damit verbundenen Dienstes entstehen, nur auf der Grundlage einer vertraglichen Vereinbarung mit dem Nutzer verwenden. Nach dieser Vorschrift ist eine Datenlizenz, also eine ausdrückliche Erklärung des Nutzers zur Nutzung der Daten durch den Dateninhaber, erforderlich. In der Praxis dürfte dieses Erfordernis in seinen Auswirkungen durch das fehlende Koppelungsverbot abgemildert werden. Unternehmen (Dateninhaber) können die Erbringung ihrer Leistungen davon abhängig machen, dass der Nutzer seine Einwilligung zur Nutzung der Daten durch den Dateninhaber erklärt. Der Entwurf verhält sich zwar nicht ausdrücklich zu der umstrittenen Thematik des „Dateneigentums“, jedoch erkennt er durch die Regelungen zum freien Datenzugang des Nutzers und dem Erfordernis einer Einwilligung desselben in die Nutzung durch andere Beteiligte dem Nutzer eine gewisse Exklusivitätsstellung zu.[4]

Einschränkungen erfährt der Datenzugang für staatliche Stellen: Der öffentliche Sektor kann nur bei einem „außergewöhnlichen Bedarf“ auf Daten zugreifen, insbesondere um auf einen öffentlichen Notfall zu reagieren oder gesetzliche Verpflichtungen zu erfüllen. In solchen Notfällen sollen die Daten der öffentlichen Stelle unentgeltlich zur Verfügung gestellt werden, während der Dateninhaber in anderen Fällen eine Entschädigung in Höhe der tatsächlich anfallenden Kosten verlangen kann.

1 MMR-Aktuell 2022, 446901; Bomhard/Merkle, RDi 2022, 168 (170).
2 Bomhard/Merkle, RDi 2022, 168 (171).
3 Bomhard/Merkle, RDi 2022, 168 (172).
4 Bomhard/Merkle, RDi 2022, 168 (175).

Die Anträge auf Zugang zu bzw. die gemeinsame Nutzung von den Daten sollen verhältnismäßig sein und nicht zum Nachteil des Dateninhabers erfolgen. Die öffentliche Stelle darf die erhaltenen Daten nicht wiederverwenden, könnte sie aber für die wissenschaftliche Forschung zur Verfügung stellen.

III. Besonderheiten für kleine und mittlere Unternehmen (KMU)

Die Verpflichtungen des Data Act gelten nicht für Daten, die durch die Nutzung von Produkten erzeugt werden, die von Unternehmen, die als KMU gelten, hergestellt oder damit verbundene Dienstleistungen erbracht werden, es sei denn, diese Unternehmen sind „wirtschaftlich von einem anderen Unternehmen abhängig, das nicht als KMU einzustufen ist."
Des Weiteren darf der Dateninhaber von solchen KMU für die Bereitstellung der Daten nicht mehr als den konkreten Bereitstellungsaufwand als Vergütung fordern.

Eine weitere Besonderheit stellt das Verbot unfairer vertraglicher Bedingungen gegenüber KMU dar. Nach der Regelung des Entwurfs müssen die Vertragsklauseln fair, angemessen und nichtdiskriminierend sein, andernfalls werden sie als nichtig betrachtet. Die vertragliche Abrede ist unbillig, wenn sie in grober Weise und entgegen Treu und Glauben von den Geschäftsgepflogenheiten abweicht. Die Regelung ähnelt hier einer AGB-Kontrolle und beschränkt die Vertragsfreiheit der Parteien. Des Weiteren wird die Beweislast umgekehrt: Wenn das andere Unternehmen die Bedingungen für diskriminierend hält, obliegt es dem Inhaber der Daten, zu beweisen, dass keine solche Diskriminierung vorliegt.

IV. Cloud-Switching, Interoperabilität und weitere Regelungen

Der Entwurf sieht die Verpflichtung zu einem umfassenden und kostenlosen Exit-Management vor. Im Ergebnis bedeutet dies, dass Verträge Klauseln zur Unterstützung des Wechsels der Nutzer zu anderen Services, Interoperabilitätsanforderungen und eine Übergangsfrist enthalten müssen. Die Anbieter von Datenverarbeitungsdiensten dürfen für den Wechsel der Nutzer keine Gebühren verlangen. Des Weiteren müssen sie die Kompatibilität mit offenen Standards oder Interoperabilitätsschnittstellen für alle anderen Dienste gewährleisten. Eine einschneidende Neuerung stellt die Regelung des Entwurfs dar, nach der Nutzer ihre Verträge jederzeit, mit einer Kündigungsfrist von maximal 30 Tagen, kündigen können. Dies schränkt die kommerzielle Planbarkeit von Cloud-Anbietern erheblich ein.

Die Kommission wird nun europäische Normungsorganisationen auffordern, harmonisierte Normen für die Interoperabilität von Cloud-Diensten auszuarbeiten. Falls dies nicht ausreichen sollte, könnte die EU-Exekutive einen Durchführungsrechtsakt erlassen, der gemeinsame Spezifikationen, offene Standards oder offene Schnittstellen vorschreibt.

Bezüglich der Vollstreckung der Verpflichtungen aus dem Data Act sieht der Entwurf vor, dass die Durchsetzung in den Händen der von den Mitgliedstaaten geschaffenen zuständigen Behörden liegt, und die Sanktionen ebenfalls auf nationaler Ebene festgelegt werden sollen.

V. Kritik und Ausblick

Erklärtes Ziel des Data Act ist es, „mehr Mitsprache" für Unternehmen und Nutzer zu erwirken, sowie mächtige Konzerne, wie Google und Meta, in ihrer Datenmonopolstellung zu schwächen. Von Experten wird hinterfragt, ob die Vorschläge des Entwurfs ausreichend sind, damit Daten in Europa künftig nicht nur dem (wirtschaftlichen) Profit von Unternehmen, sondern auch dem Gemeinwohl dienen.

Kritisiert wird zum einen die nur beschränkte Zugriffsmöglichkeit der öffentlichen Hand. Zum anderen enthält der Entwurf einige Unsicherheitsfaktoren, wie beispielsweise die Einordnung von Produkten unter den Anwendungsbereich des Data Act, die genaue Zuordnung von Daten zu einzelnen Nutzern sowie das Zusammenspiel des Data Act mit dem Datenschutz- und Kartellrecht. Das weitere Gesetzgebungsverfahren sollte nun genutzt werden, um diese Unklarheiten auszuräumen.

Zuletzt ist mit Blick in die Zukunft zu fragen, wann mit dem Inkrafttreten der einschneidenden Änderungen im Bereich des Datenzugangs und -austauschs gerechnet werden kann: Der Kommissionentwurf wird nun durch das Europäische Parlament und den Rat der EU gehen. Erfahrungsgemäß kann es ca. zwei Jahre dauern, bis eine derartige Verordnung ratifiziert wird und in Kraft tritt, teilweise auch deutlich länger. Der Entwurf selbst sieht einen Übergangszeitraum von 12 Monaten nach dem

formellen Inkrafttreten vor. Das bedeutet, dass die materielle unmittelbare Geltung der Verordnung aufgeschoben wird und den Mitgliedsstaaten eine Schonfrist zur Umstellung und Anpassung an die Vorgaben der Verordnung bleibt. Im frühesten Falle ist daher im Jahr 2025 eine Geltung des Data Act zu erwarten.[5]

VI. Fazit und Bedeutung für Hochschulen

Der Data Act entfaltet Relevanz für Hochschulen als Teil der öffentlichen Hand. Ihnen steht ein Recht auf Zugang zu Daten nur im Ausnahmefall unter besonderen Bedingungen zu. Soweit es sich um private Institutionen handelt, finden (je nach Größe) die übrigen Regelungen des Entwurfs zum Datenzugang und -austausch, sowie gegebenenfalls die Modifikationen für KMU Anwendung.

Die Zielsetzung des Entwurfs kommt grundsätzlich auch den Hochschulen und der Wissenschaft zugute. Ein umfassender Zugang zu und Austausch von nicht-personenbezogenen Daten kann nicht nur die Wirtschaft, sondern auch Wissenschaft und Forschung vorantreiben. Nachteilig und daher zu Recht zu hinterfragen ist jedoch die beschränkte Datenzugangsmöglichkeit für den staatlichen Sektor.

5 Bomhard/Merkle, RDi 2022, 168 (176).

Geheim bis das Erbe uns scheidet

Der neue § 4 TTDSG und seine Auswirkungen auf den digitalen Nachlass

von Owen Mc Grath

Das Thema digitaler Nachlass hat in den vergangenen Jahren in der juristischen Welt immer wieder für Furore gesorgt. Auch im DFN-Infobrief wurde hierzu schon mehrmals berichtet.[1] Nun hat sich auch der deutsche Gesetzgeber dem Thema angenommen und mit § 4 Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) Teile der bisherigen Rechtsprechung des Bundesgerichtshofs (BGH) in Gesetzesform gegossen. Grund genug, sich die neue Regelung im Detail anzusehen. Denn die Relevanz ist auch für Hochschulen nach wie vor hoch.

I. Entscheidungen zum digitalen Nachlass

Den maßgeblichen Entscheidungen des BGH zum digitalen Nachlass liegt ein dramatischer Sachverhalt zugrunde. Die Eltern eines verstorbenen Kindes verlangten von Facebook Zugriff auf das Konto des Kindes, wogegen sich Facebook wehrte. Der Fall landete schließlich beim BGH, der 2018 zugunsten der Eltern des Kindes entschied (Az. III ZR 183/17). Sie erhielten beschränkten Zugriff auf das Konto ihrer verstorbenen Tochter. Im Jahr 2020 war der BGH erneut mit dem Fall befasst und entschied diesmal zum Umfang des Zugriffsrechts der Eltern (Az. III ZB 30/20). Wieder unterlag Facebook. Das Unternehmen musste den Eltern in der Folge den vollen Zugriff auf den Account der Tochter gewähren. In der maßgeblichen ersten Entscheidung von 2018 ging der BGH davon aus, dass der Nutzungsvertrag zwischen dem Kind und Facebook beim Tod gem. § 1922 Bürgerliches Gesetzbuch (BGB) auf ihre Erben, hier also die Eltern, übergegangen sei. Damit erkannte der BGH erstmals den sog. „digitalen Nachlass“ höchstrichterlich an. Im Zuge dieser Entscheidung setzte sich der BGH auch mit der Frage auseinander, ob das grundgesetzlich in Art. 10 GG verankerte Fernmeldegeheimnis dem Zugangsanspruch der Erben im Weg stehen könnte. Vereinfacht gesagt schützt das Fernmeldegeheimnis ähnlich dem Briefgeheimnis digitale Kommunikationsvorgänge. Im konkreten Fall ging es um die Frage, ob § 88 Abs. 3 S. 1 Telekommunikationsgesetz (TKG) a. F. dem Diensteanbieter untersagt, den Erben Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Der BGH verneinte dies und führte zur Argumentation aus, § 88 Abs. 3 S. 1 TKG a. F. schütze nur vor Kenntnisnahme durch am Kommunikationsvorgang nicht Beteiligte. Mit Eintritt des Erbfalls seien die Eltern aber nicht mehr Unbeteiligte, sondern träten an die Stelle der Erblasserin, also der Tochter. Im Ergebnis stand das Fernmeldegeheimnis dem Zugangsanspruch der Eltern somit nicht entgegen.

II. Umsetzung im TTDSG

Trotz dieser höchstrichterlichen Klärung sah sich der Gesetzgeber zu einer gesetzlichen Regelung aufgefordert. Das am 1.Dezember 2021 in Kraft getretene TTDSG bot hierfür eine gute Gelegenheit. Das Fernmeldegeheimnis, wie es heute in § 3 Abs. 1 TTDSG ausbuchstabiert ist, schützt den Inhalt der Telekommunikation und ihre näheren Umstände. Verpflichtet, das Fernmeldegeheimnis zu wahren, sind insbesondere „Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken“, wie sich aus § 3 Abs. 2 Nr. 1 TTDSG ergibt. § 4 TTDSG sieht nun eine Einschränkung des Fernmeldegeheimnisses im Sinne der obigen Rechtsprechung des BGH vor. § 4 TTDSG normiert, dass das Fernmeldegeheimnis der Wahrnehmung von Rechten gegenüber dem Anbieter des Telekommunikationsdienstes nicht entgegensteht, „wenn diese Rechte statt durch den betroffenen Endnutzer durch seinen Erben oder eine andere berechtigte Person, die zur Wahrnehmung der Rechte

1 Tiessen, Der lange Weg zum letzten Willen, DFN-Infobrief Recht 11/2020; Strobel, Digitaler Nachlass – letzter Akt, DFN-Infobrief Recht 9/2018.

des Endnutzers befugt ist, wahrgenommen werden".
Die Überführung der Rechtsprechung des BGH in Gesetzesform ist durchaus begrüßenswert, wirft aber auch neue Fragen auf.

III. Einzelfragen

Grundsätzlich ist festzuhalten, dass § 4 TTDSG dem gesetzgeberischen Willen nach Klarstellung und damit der Rechtssicherheit dienen soll. Der Gesetzgeber wollte vornehmlich die Rechtsprechung des BGH kodifizieren und einige bisher unbeantwortete Rechtsfragen klären.

Die Norm sieht eine Begrenzung des Fernmeldegeheimnisses zunächst für den Fall vor, dass die Rechte gegenüber dem Anbieter des Telekommunikationsdienstes statt durch den betroffenen Endnutzer durch seinen Erben wahrgenommen werden. Insoweit spiegelt die Norm die bisherige Rechtsprechung wieder.

Darüber hinaus ist das Fernmeldegeheimnis aber auch begrenzt, wenn die Rechte der betroffenen Person durch „eine andere berechtigte Person, die zur Wahrnehmung der Rechte des Endnutzers befugt ist, wahrgenommen werden". Hinter den anderen berechtigten Personen verbergen sich laut der Gesetzesbegründung zunächst der Testamentsvollstrecker, Nachlasspfleger, Nachlassverwalter und der Nachlassinsolvenzverwalter. Das ist insofern stimmig, als auch diese Personen ein berechtigtes Interesse an der Wahrnehmung von Kommunikationsinhalten haben können. In diesen Personenkreis kann darüber hinaus auch noch ein zu Lebzeiten bestellter Betreuer fallen, oder eine Person, die durch den Endnutzer mit entsprechender Vertretungsmacht ausgestattet wurde. An dieser Stelle geht § 4 TTDSG über die bisherige Rechtsprechung des BGH hinaus. Denn dieser hatte von § 88 Abs. 3 S. 1 TKG a.F. lediglich die Erben ausgenommen, nicht aber andere Personen.

Keinen Einfluss hat § 4 TTDSG hingegen auf die Frage, inwiefern der Erblasser seinen digitalen Nachlass im Wege einer letztwilligen Verfügung regeln kann. Der Erblasser kann seinen digitalen Nachlass im Rahmen seiner Testierfreiheit also weiterhin frei ausgestalten: er kann den Kreis der berechtigten Personen beschränken, den Umfang, in dem seine Rechte gegen den Diensteanbieter auf diese übergehen oder andere Anordnungen treffen. Das ergibt sich aus dem nur klarstellenden Charakter der Norm. Der Gesetzgeber hat mit § 4 TTDSG die Testierfreiheit des Erblassers nicht einschränken wollen.

IV. Praxishinweise für Hochschulen

Auch Hochschulen können durch die neue Regelung des § 4 TTDSG betroffen sein. Die Norm richtet sich an Anbieter von Telekommunikationsdiensten. Das ist nach § 2 Abs. 1 TTDSG i.V.m. § 3 Nr. 1 TKG jeder, der Telekommunikationsdienste erbringt. Betroffen sein können aber nur die in § 3 Abs. 2 S. 1 TKG genannten Personen, da auch nur diese zur Wahrung des Fernmeldegeheimnisses überhaupt verpflichtet sind. Insbesondere sind damit „Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken" umfasst. Das wird auch auf Hochschulen und Forschungseinrichtungen regelmäßig zutreffen. Praxisrelevant könnte § 4 TTDSG beispielsweise werden, wenn die Erben eines verstorbenen Hochschulmitglieds Zugang zu dessen hochschuleigenen E-Mail-Konto begehren. Die Hochschule muss sich dann, zumindest für die nicht dienstlichen Inhalte, nach dem neuen § 4 TTDSG und damit auch der Rechtsprechung des BGHs richten. Sollte sich eine Hochschule einem solchen Verlangen ausgesetzt sehen, ist zunächst wichtig, die Berechtigung des Anspruchstellers genau zu überprüfen. Der Kreis der Berechtigten ist oben erläutert worden. Gewährt eine Hochschule einem Nichtberechtigten Zugang, verstößt sie damit gegen das Fernmeldegeheimnis. Schon deshalb darf sich nicht auf eine reine Behauptung verlassen werden, sondern die Berechtigung nachgewiesen und –geprüft werden. Erben können hierzu unter anderem das Testament oder Personenstandsurkunden vorlegen, der Testamentsvollstrecker das Testamentsvollstreckerzeugnis. Nachlasspfleger, -verwalter, und Nachlassinsolvenzverwalter können ihre Bestallungsurkunde zum Nachweis vorlegen. Teilweise ist auch auf den Umfang der Berechtigung zu achten. Das ist insbesondere beim Betreuer oder Vorsorgebevollmächtigten der Fall. Die von ihnen vorgebrachten Nachweise müssen gerade auch ihre Berechtigung zur Geltendmachung der Rechte des Erblassers gegen den Anbieter des Telekommunikationsdienstes umfassen. Steht der Wille des Erblassers dem nicht entgegen, muss die Hochschule dem Berechtigten sodann den Zugang zu den Kommunikationsinhalten gewähren. Dabei genügt es nicht, dass nur Kopien der Nutzerkontoinhalte zur Verfügung gestellt wurden. Der BGH hat in seiner zweiten Entscheidung im Jahr 2020 explizit entschieden, dass der Zugang zum Konto selbst gewährt werden muss. Die Erben müssen sich im Konto des Erblassers so bewegen können, wie der Erblasser selbst es konnte. Nicht erforderlich ist hingegen, dass den Erben die aktive Nutzung des Kontos ermöglicht wird. Es genügt die Überlassung im Sinne eines „read-only"-Zugangs.

V. Fazit

Werden die obenstehenden Hinweise beachtet, ist für Hochschulen ein rechtssicherer Umgang mit dem digitalen Nachlass möglich. Insofern stellt § 4 TTDSG eine willkommene Klärung dar, die zur Rechtssicherheit aller Beteiligten beiträgt. Das Thema digitaler Nachlass ist damit aber nicht erschöpfend geklärt. Es lohnt sich, die weitere Rechtsentwicklung im Blick zu behalten.

Brüssel reguliert das schon

EU-Institutionen einigen sich final auf DMA und DSA

von Justin Rennert

Die EU-Institutionen haben sich im März und April auf endgültige Gesetzestexte für den Digital Markets Act (DMA) und den Digital Services Act (DSA) geeinigt. Die Einigung steht am Ende vergleichsweise zügiger Verhandlungen. Dies zeigt, wie wichtig der EU eine umfassende Regulierung von Online-Diensteanbietern ist. Wir werfen einen Blick auf die endgültigen Gesetzestexte.

I. Hintergrund der Gesetzgebungsverfahren

„For me, the most exciting thing in the software area is the internet. And part of the reason is: No one owns it. The rate of innovation is very high. We know from experience now that if any one company gets a dominant position in it [JR: the internet], no matter who that is, the rate of innovation is going to drop precipitously. And we'd like to not see this happen forever - or at least for quite some time." Dieses Zitat stammt von Apple-Mitgründer Steve Jobs aus dem Jahre 1996. Damals, wenige Monate bevor er nach über zehnjähriger Abwesenheit in den Vorstand von Apple zurückkehrte, sah Steve Jobs eine Hauptgefahr für Innovationen im Internet: dass ein einzelnes Unternehmen dort eine marktbeherrschende Stellung erlangt. „Forever - or at least for quite some time". Der letzte Halbsatz ist bezeichnend, denn ironischerweise ist nun genau das von Jobs gegründete Unternehmen Apple eines der Big-Four-in-Tech, das die Spielregeln in der Online-Welt mitdiktiert. Ist die Zeit also nun reif für einige wenige Unternehmen mit marktbeherrschender Stellung?

Die EU-Institutionen Kommission, Ministerrat und Parlament sehen dies nicht so. Stattdessen möchten sie die Marktmacht großer Online-Konzerne beschränken. Im Dezember 2020 veröffentlichte die EU-Kommission daher einen ersten Entwurf eines Digital Markets Act, kurz DMA. Der DMA soll in der gesamten EU für faire digitale Märkte sorgen. Seine Vorschriften sind dabei nur auf einige wenige Online-Plattformen anwendbar – eben nur auf solche, die eine besondere Marktmacht innehaben. In für EU-Verhältnisse hoher Geschwindigkeit passierte der DMA die informellen Trilog-Verhandlungen zwischen EU-Parlament, Ministerrat und Kommission. Am 23. März 2022 konnten die EU-Institutionen eine endgültige Einigung verkünden. Mit einem Inkrafttreten des Gesetzespaketes ist Anfang 2023 zu rechnen – anwendbar wird der DMA aufgrund von Übergangsvorschriften wohl aber erst ab dem Jahre 2024 sein.

Der DMA bildet jedoch nur die erste Hälfte der ambitionierten EU-Vorhaben zur Internetregulierung. Die andere Hälfte bildet der sog. Digital Services Act, kurz DSA. Der DSA erfasst deutlich mehr Unternehmen als der DMA und schafft Haftungs- und Sicherheitsvorschriften für eine große Vielzahl an Online-Diensten, nicht nur solche mit besonderer Marktmacht. Der DSA soll nach dem Willen der EU-Kommission für ein sicheres, berechenbares und vertrauenswürdiges Online-Umfeld sorgen. Auf den DSA einigten sich die EU-Institutionen in ähnlich schneller Geschwindigkeit wie auf den DMA.[1] Am 23. April 2022 konnten Parlament und Rat hier die Einigung im informellen Trilog-Verfahren verkünden. Kommissionspräsidentin Ursula von der Leyen bezeichnete den Schritt daraufhin auf Twitter als „historisch". Mit einer Geltung der DSA-Vorschriften kann ebenfalls ab Anfang 2024 gerechnet werden.

Bei beiden Gesetzespaketen handelt es sich um Verordnungen. Anders als EU-Richtlinien sind diese unmittelbar in der gesamten EU anwendbar und bedürfen keiner Umsetzung durch die nationalen Gesetzgeber der Mitgliedsstaaten. Das unterstreicht die

1 Zum ersten Entwurf der EU-Kommission von Ende 2020: Gielen, „Digital Services Act: Das Plattformgrundgesetz?" in: DFN-Infobrief Recht 03/2021.

Wichtigkeit, die die EU den Regelungsvorhaben beimisst. Beide Gesetzespakete müssen nun noch formal von EU-Ministerrat und EU-Parlament gebilligt werden. Dabei handelt es sich jedoch nur um Formalitäten. Dass die Gesetzespakete in Kraft treten, ist nach der politischen Einigung ausgemachte Sache. Zeit für uns, einen Überblick über die Regelungen der Gesetzespakete zu werfen.

II. Der DMA: Ein Regelwerk für Gatekeeper

Der DMA richtet sich an Unternehmen, die den Zugang zu Internetplattformen wie eine Art Türsteher, also „Gatekeeper", kontrollieren. Das Gesetz spricht insofern selbst von „Gatekeeper", auch in der deutschen Fassung. Wer genau unter diese Definition fällt, wurde nun in einem abschließenden Kompromiss des Trilogs festgelegt. Betroffen sind Unternehmen mit einer Marktkapitalisierung von mindestens 75 Milliarden Euro oder einem Umsatz im europäischen Wirtschaftsraum von mindestens 7,5 Milliarden Euro. Zudem müssen die Plattformen 45 Millionen monatliche Nutzer in der EU und 10.000 aktive geschäftliche Nutzer pro Jahr haben. Die Plattform muss zudem in mindestens drei Mitgliedstaaten einen oder mehrere zentrale Plattformdienste betreiben, also etwa soziale Netzwerke, Webedienste, Browser, Suchmaschinen oder Marktplätze.

Doch ein Unternehmen hat die Regeln des DMA nicht automatisch zu befolgen, sobald es die oben genannten Kriterien erfüllt. Die EU-Kommission muss ein Unternehmen aktiv und formal als „Gatekeeper" benennen. Erst dann hat das Unternehmen die Regeln des DMA zu befolgen. Vor dieser Benennung trifft ein Unternehmen lediglich eine Mitteilungspflicht an die EU-Kommission. Es muss laufend prüfen, ob es die oben genannten Schwellenwerte (also: 75 Mrd. Marktkapitalisierung oder 7,5 Milliarden Umsatz) erreicht. Wenn dem so ist, muss eine Mitteilung an die EU-Kommission gemacht werden. Diese prüft dann, ob die übrigen Voraussetzungen für die Benennung als Gatekeeper vorliegen.

Ist eine solche formale Benennung erfolgt, sieht der DMA eine Reihe von Verhaltenspflichten für die erfassten Unternehmen vor. Hierunter fällt zum Beispiel das Gebot der Interoperabilität für Messengerdienste. Gatekeeper müssen zukünftig ihre Dienste so gestalten, dass sie mit Diensten von anderen Unternehmen kompatibel sind. Ein einfaches Beispiel: Über 90 Prozent der unter 30-jährigen nutzen WhatsApp. WhatsApp muss aufgrund des DMA zukünftig ermöglichen, dass auch Nutzer anderer Messengerdienste Nachrichten an WhatsApp-Nutzer schicken können – und umgekehrt: zumindest technisch soll WhatsApp die Möglichkeiten schaffen, dass man als WhatsApp-Nutzer beispielsweise einem Signal-Nutzer eine Nachricht schicken kann. Diese strenge Interoperabilitätspflicht gilt aber nach dem endgültigen Entwurf nur für Messengerdienste, nicht für soziale Netzwerke. Ob die Interoperabilität auch auf soziale Netzwerke ausgedehnt werden soll, war bis zuletzt ein großer politischer Streitpunkt.

Generell ist der DMA sehr von dem Interoperabilitätsgedanken geprägt. Ein weiteres Gebot, das in diesem Zuge zu nennen ist: Anbieter von Betriebssystemen müssen zukünftig auch App-Stores anderer Anbieter zulassen. Zudem verbietet der DMA explizit, dass Gatekeeper eigene Produkte und Angebote gegenüber solchen der Konkurrenz bevorzugen. Zum Beispiel muss es zukünftig möglich sein, dass Nutzer eines Smartphone-Betriebssystems vorinstallierte Apps löschen können.

Neben dieser kartell- und regulierungsrechtlichen Dimension enthält der DMA jedoch auch datenschutzrechtliche Vorschriften: Zu den verbotenen Verhaltensweisen zählt zum Beispiel die Kombinierung personenbezogener Daten aus einem bestimmten Plattformdienst mit solchen aus anderen Diensten desselben Konzerns, es sei denn, der Nutzer hat ausdrücklich eingewilligt. Dies soll die Bildung von umfassenden Persönlichkeitsprofilen verhindern. Denn das Bild, das ein Gatekeeper von seinen Nutzern hat, ist umso genauer, je verschiedenartiger die Dienste sind, bei dessen Nutzung er die Daten erhoben hat.

III. Der DSA: Ein Regelwerk für das ganze Internet

„Der DSA soll dafür sorgen, dass das, was offline illegal ist, auch online illegal ist". So äußerte sich EU-Kommissionspräsidentin Ursula von der Leyen im Zuge der politischen Einigung auf das endgültige Regelwerk. Der DSA ist ein Sammelwerk an Vorschriften, die den Regulierungsrahmen für das Internet bereit für die 20er Jahre machen sollen. Die bisher einschlägigen Vorschriften der eCommerce-RL stammen schließlich noch aus dem Jahr 2000. Das Gesetz selbst spricht davon, dass es „einheitliche Regeln für ein sicheres, vorhersehbares und vertrauenswürdiges Online-Umfeld festlegen möchte", in der die EU-Grundrechtecharta wirksam geschützt wird.

Der Anwendungsbereich des DSA ist dementsprechend deutlich weiter als der des DMA. Er umfasst verschiedene Online-Vermittlungsdienste, die sich unterteilen lassen in reine Durchleiter, Caching-Dienste und Hosting-Dienste. Unter erstere fallen beispielsweise Telekommunikations-Diensteanbieter. Die Caching-Dienste sind solche, die die von einem Nutzer bereitgestellte Information zum Zwecke der Übermittlung der Information zwischenspeichern. Den breitesten Anwendungsbereich haben die Hosting-Dienste. Darunter fallen Betreiber sozialer Netzwerke, Suchmaschinen, Betreiber von App-Stores und Marktplätze. Diese werden auch am stärksten reguliert, wobei sehr große Online-Plattformen und -Suchmaschinen sogar noch strengeren Anforderungen unterworfen werden.

Ein zentraler Aspekt der Regulierung von Hosting-Plattformen ist die Content-Moderation. Der DSA sieht vor, dass Diensteanbieter ein Meldesystem einrichten, dem die Nutzer aus ihrer Sicht illegale Inhalte melden können. Die Verfahren müssen leicht zugänglich und benutzerfreundlich sein. Im Falle einer Entfernung oder Sperrung des Inhalts, muss der Betroffene umfassend über die Gründe der Sperrung aufgeklärt werden. Online-Plattformen müssen darüber hinaus ein internes Beschwerdemanagement einrichten, worüber eine Löschung oder Sperrung des Inhalts, die Suspendierung eines Nutzers oder sogar die Löschung des Nutzerkontos erfolgen kann.
In Deutschland ist eine ähnliche Pflicht zur internen Content-Moderation in Gestalt des Netzwerkdurchsetzungsgesetzes (NetzDG) schon geltendes Recht. Der wichtigste Unterschied ist der folgende: Während das NetzDG nur eine Moderation im Hinblick auf bestimmte Strafgesetze vorsieht, führt der DSA die Pflicht ein, sämtliche rechtswidrige Inhalte zu moderieren. Dies umfasst grundsätzlich die gesamte Rechtsordnung.

Doch die plattforminterne Content-Moderation ist nicht der einzige Weg, um illegale Inhalte zu bekämpfen. Der DSA sieht auch vor, dass die Behörden der Mitgliedsstaaten Host-Providern ohne vorherige Befassung eines Richters Anordnungen schicken dürfen, dass bestimmte illegale Inhalte zu blockieren sind. Diese Inhalte sind dann „ohne unangemessene Verzögerung zu sperren oder zu blockieren".
Doch die Regeln des DSA sind vielfältig: Das Gesetz sieht beispielsweise auch eine Haftungsbefreiung für reine Durchleitungsdienste vor. So sollen Telekommunikationsdiensteanbieter für in ihren Netzen übermittelte Informationen dann nicht haften, wenn er die Übermittlung nicht veranlasst hat, den Adressaten der übermittelten Information nicht auswählt und die übermittelten Informationen nicht auswählt oder inhaltlich verändert. In Deutschland ist diese Haftungsbefreiung in Gestalt des § 8 TMG freilich schon geltendes Recht.
Ein weiterer politischer Streitpunkt war das Verbot der personalisierten Werbung. In seiner endgültigen Fassung soll der DSA ein Verbot personalisierter Werbung nur gegenüber Minderjährigen vorsehen. Diensteanbieter dürfen personenbezogene Daten von Minderjährigen also überhaupt nicht mehr verwenden, um diesen personalisierte Werbung anzuzeigen. Bei volljährigen Personen dürfen Dienstenabieter lediglich keine besonders sensiblen Daten auswerten (also z.B. Gesundheitsdaten oder Daten zur sexuellen Orientierung).

IV. Fazit und Bedeutung für Hochschulen

Die praktische Bedeutung von DMA und DSA kann nicht überbetont werden. Sind die Regeln erst einmal in Kraft, so wirken sie sich auf nahezu jeden Internetnutzer und dementsprechend auch auf Angehörige von Hochschul- und Forschungseinrichtungen aus. Bei Hochschulen und Forschungseinrichtungen handelt es sich nicht um Gatekeeper im Sinne des DMA. Allerdings können sie durchaus unter die Regeln des DSA fallen. Dessen Anwendungsbereich ist deutlich weiter. Es ist beispielsweise denkbar, dass eine Hochschule „Hosting-Dienst" im Sinne des DSA ist – und zwar wenn sie Nutzern auf einer eigenen Webseite ermöglicht, eigene Inhalte hochzuladen (beispielsweise bei Betrieb von Online-Lernplattformen).
Besonders interessant für Forscherinnen und Forscher ist zudem die Vorschrift des Art. 31 Abs. 2 des DSA. Danach müssen sehr große Online-Plattformen Forschenden auf Anfrage in gewissen Fällen Zugang zu eigenen nichtöffentlichen Daten geben. Es handelt sich hierbei zum Beispiel um Informationen über die von Plattformen eingesetzten Algorithmen. Die Auswertung der Daten soll ein besseres Verständnis der systemischen Risiken sehr großer Online-Plattformen liefern.[2]
Doch die Regeln des DMA und DSA sind nicht nur von unmittelbarer Relevanz. Auch mittelbar wirken sie sich auf Hochschulen und Forschungseinrichtungen aus. Viele Drittanbieterdienste (z. B. Analytics-Plattformen) sind zum gegenwärtigen Zeitpunkt nicht DMA- und DSA-konform. Hier sollten Hochschulen und Forschungseinrichtungen künftig darauf achten, nur rechtskonforme Drittanbieterdienste einzusetzen.

2 Ausführlich: Gielen, „Digital Services Act: Das Plattformgrundgesetz?" in: DFN-Infobrief Recht 03/2021.

Kurzbeitrag: Künast die Dritte

Die Entscheidung des Landgerichts Frankfurt am Main zur Sperrpflicht von Meta

von Johanna Schaller

Nachdem Ende des letzten Jahres bereits das Bundesverfassungsgericht in Sachen Renate Künast gegen Facebook ein Machtwort gesprochen hat[1], hat nun das Landgericht (LG) Frankfurt in einem anderen Verfahren zu der Sperrpflicht Metas bei der Verbreitung von Falschzitaten auf der Plattform Facebook Stellung genommen.

I. Hintergrund[1]

Auf der Plattform Facebook, einem sozialen Netzwerk des Unternehmens Meta, wurde ein Bild von Renate Künast mitdem folgenden Zitat veröffentlicht: „Integration fängt damit an, dass Sie als Deutscher mal türkisch lernen!“ Dass Renate Künast diesen Satz nicht gesagt hat und es sich somit um ein sogenanntes Fake-Zitat handelt, war schon lange geklärt. Der Beitrag mit dem Zitat wurde in der folgenden Zeit in verschiedenen Varianten durch „Hochladen“ (Uploads) und „Teilen“ verbreitet, etwa mit verändertem Layout oder durch Erweiterung oder Weglassen von Textinhalten. Diese Varianten haben eine andere URL als die ursprüngliche Wort-Bild-Kombination (sog. „Meme“). Zwar kann die Politikerin die neuen Memes in jedem einzelnen Fall bei Meta, der Betreiberin von Facebook, melden und die Löschung des konkreten Beitrags verlangen.
Mit ihrer Klage vor dem Landgericht Frankfurt am Main zielte Renate Künast nun aber darauf ab, dass Meta selbst die Pflicht trifft, nach solchen sinngleichen Posts zu suchen und diese zu löschen.

II. Sieg für Künast: Sperrpflicht und Geldentschädigung

Das LG hat der Klage der Politikerin stattgegeben und urteilte, dass der Diensteanbieter (Meta) auch Varianten des Memes des Fake-Zitats Künasts mit kerngleichem Inhalt ohne erneuten Hinweis auf die jeweilige URL löschen muss.[2]

Das allgemeine Persönlichkeitsrecht schützt sowohl vor unrichtigen, verfälschten als auch entstellten Wiedergaben einer Äußerung. Somit werde Renate Künast durch das Falschzitat in ihren Persönlichkeitsrechten verletzt. Für diese Verletzung sei Meta auch als sog. „mittelbare Störerin“ verantwortlich. Ein Diensteanbieter müsse zwar grundsätzlich nicht ohne einen Hinweis jegliche von den Nutzern ins Netz gestellte Beiträge vor der Veröffentlichung auf eine eventuelle Rechtsverletzung prüfen. Nach dem konkreten Hinweis der Betroffenen darauf„ dass die ihr zugeschriebene Äußerung ein falsches Zitat ist, ist der Diensteanbieter nicht nur dazu verpflichtet, den konkreten Inhalt unverzüglich zu sperren, sondern hat auch Vorsorge zu treffen, dass es möglichst nicht zu weiteren gleichartigen Rechtsverletzungen kommt. Frau Künast müsse diesen Hinweis dann auch nicht für jeden weiteren Rechtsverstoß unter Angabe der URL wiederholen.[3] Ferner sei es Meta auch technisch und wirtschaftlich zumutbar, auch ohne konkrete Bezeichnung der URL, identische und ähnliche Memes, mittels Vergleich der sogenannten „Hashwerte“ zu erkennen. Das Gericht legt somit der Betreiberin des sozialen Netzwerks die Pflicht auf, selbst festzustellen, ob in einer ihm bekannten Abwandlung („Meme“) das Charakteristische der konkreten Verletzungsform zum Ausdruck kommt und damit kerngleich ist.

Des Weiteren sprach das Gericht Renate Künast wegen der Verletzung ihres allgemeinen Persönlichkeitsrechts eine

1 Schaller, Machtwort gegen Hass und Hetze, DFN-Infobrief Recht 04/2022; Tiessen, Sag mir deinen Namen und ich sag dir, was du bist – LG Berlin zu Auskunftsansprüchen wegen Beleidigung auf Social Media-Plattformen, DFN-Infobrief Recht 5/2020.

2 LG Frankfurt a. M. vom 08.04.2022 – 2-03 O 188/21: https://www.lareda.hessenrecht.hessen.de/bshe/document/LARE220002783.

3 https://ordentliche-gerichtsbarkeit.hessen.de/pressemitteilungen/ehrverletzung-durch-falschzitat-in-sozialem-netzwerk.

Geldentschädigung in Höhe von 10.000 Euro gegen Meta zu. Das Unternehmen sei seiner Verpflichtung nicht nachgekommen, die Plattform Facebook von weiteren Falschzitaten zu befreien. Aufgrund dieser Mitverantwortung Metas und der Schwere der Persönlichkeitsrechtsverletzungen sei das Schmerzensgeld gerechtfertigt. Renate Künast sei aufgrund der Falschzitate Anfeindungen ausgesetzt gewesen. Solche Falschzitate seien nach der Begründung des Gerichts geeignet die Glaubwürdigkeit der Politikerin zu beschädigen, den Meinungskampf zu verzerren und der Allgemeinheit zu schaden.

III. Bedeutung für Hochschulen

Nicht nur Private und Politiker, sondern auch Hochschulen und Angehörige derselben sind heutzutage regelmäßig auf sozialen Netzwerken, wie beispielsweise Facebook, mit einem Profil vertreten. Das Urteil stärkt die Rechte der Betroffenen und nimmt Meta in die Pflicht, selbst tätig zu werden und bei Verletzungen des allgemeinen Persönlichkeitsrechts Geldentschädigungen zu leisten. Wie schon die Besprechung der Entscheidung des Bundesverfassungsgerichts zeigte, nimmt die enthemmte Kommunikation im Netz immer weiter zu. Die Betroffenen haben nur eingeschränkte Möglichkeiten, sich gegen die Angriffe gegen sie zu verteidigen. Eine Konkretisierung und Ausweitung der Prüf- und Löschpflichten der Betreiber der sozialen Netzwerke ist daher zu befürworten.

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