



Links rein, dann rechtlich raus?!

Bundesgerichtshof äußert sich erneut zur Haftung für Hyperlinks

Privilegierte Störer?

Bundestag beschließt Gesetz zur Haftung von WLAN-Betreibern

Alles neu macht der Mai?!

Grundsätze für die Verarbeitung personenbezogener Daten nach der Datenschutz-Grundverordnung

Links rein, dann rechtlich raus?!

Bundesgerichtshof äußert sich erneut zur Haftung für Hyperlinks

von Clara Ochsenfeld

Der Bundesgerichtshof (BGH) hat in einer am 18. Juni 2015 ergangenen Entscheidung (Az.: I ZR 74/14) seine Rechtsprechung zur Haftung für Hyperlinks erneut konkretisiert. Ein Webseiten-Anbieter haftet demnach nur dann für einen Link, der zu einer fremden Seite mit rechtswidrigen Inhalten führt, wenn die Rechtswidrigkeit des Inhalts auf der verlinkten Seite für ihn deutlich erkennbar war oder er auf die Rechtswidrigkeit explizit hingewiesen wurde, sofern er sich den fremden Inhalt nicht schon zu Eigen gemacht hat. Das bloße Setzen eines Links auf der eigenen Webseite, der auf die Startseite des Internetauftrittes eines Dritten führt, genügt hierfür laut BGH jedoch gerade nicht.

Problemaufriss und Hintergrund

Der Verweis auf Inhalte Dritter durch eine Verlinkung zu einer fremden Webseite stellt eine Selbstverständlichkeit dar, die aus dem Internet nicht mehr wegzudenken ist. Mit einem einfachen „Klick“ gelangt der Nutzer zu den gewünschten verknüpften Informationen und begibt sich auf die Webseite und damit in die Sphäre eines Dritten. Die Bereitstellung von Informationen wird durch eine Verlinkung wesentlich vereinfacht, was zu einer Förderung des Informationsflusses führt. So einfach das Klicken eines Links ist, so kompliziert sind die sich aus der Nutzung von Verlinkungen ergebenden haftungsrechtlichen Fragestellungen. Dies ist darauf zurückzuführen, dass der Gesetzgeber die Haftung desjenigen, der durch einen Hyperlink den Zugang zu rechtswidrigen Inhalten eröffnet, bewusst nicht explizit geregelt hat. Folglich richtet sich das rechtliche Einsteigen für fremde Inhalte nach den allgemeinen Vorschriften. Demzufolge kommt es darauf an, ob sich derjenige, der den Link gesetzt hat, die fremden Inhalte zu Eigen gemacht hat, sodass er sich wie ein Content-Provider i.S. des § 7 Abs. 1 Telemediengesetz (TMG) behandeln lassen muss. Ein solcher bietet nämlich eigene Inhalte an, für die er in vollem Umfang haftet, sofern sie rechtswidrig sind. Darüber hinaus kann der Inhaber einer Webseite als Störer in Anspruch genommen werden, wenn es um die Verletzung absoluter, also gegenüber jedermann geltender Rechte (z. B. um eine Verletzung des Allgemeinen Persönlichkeitsrechts, des Marken- oder

Urheberrechts) geht und er die ihm auferlegten zumutbaren Prüfpflichten verletzt.

Die Gerichte haben sich in der Vergangenheit bereits in einer Vielzahl von Fällen mit der Frage befassen müssen, ob derjenige, der auf seiner Webseite durch die Bereitstellung eines Links auf die Inhalte der Seite eines Dritten verweist, für einen rechtsverletzenden Inhalt auf der Seite des Dritten rechtlich einstehen muss. Die Gerichtsentscheidungen fielen dabei je nach Einzelfall unterschiedlich aus. Grundsätzlich stellte der BGH darauf ab, ob sich derjenige, der durch einen Link auf Inhalte Dritter verweist, sich diesen Inhalt des Dritten aus objektiver Sicht eines verständigen Durchschnittsnutzers auf der Grundlage einer Gesamtbetrachtung aller relevanten Umstände zu Eigen macht, indem eine Identifikation mit der Seite des Dritten zum Ausdruck gebracht wird. Ist dies der Fall, so haftet er wie für eigene Inhalte. Auch die aktuelle Entscheidung des BGH stellt auf das Prinzip des Zueigenmachens ab, verneint es im konkreten Fall jedoch mit dem Argument, dass für den Webseitenbetreiber deutlich erkennbar sein müsse, dass auf der Webseite des Dritten Rechtsverletzungen begangen werden.

Sachverhalt der Entscheidung

Die Entscheidung des BGH erging aufgrund einer wettbewerbsrechtlichen Streitigkeit, in der ein Orthopäde auf der Webseite seiner Praxis für eine alternative Behandlungsmethode durch Implantat-Akupunktur warb. Im Zuge dessen hielt er einen empfehlenden Link mit dem Titel „Weitere Informationen über die Studienlage“ bereit, der beim Anklicken auf die Startseite der Internetpräsenz eines Forschungsverbandes führte. Auf der Webseite des Forschungsverbandes wurden Beiträge über Implantat-Akupunktur zum Abruf bereitgestellt. Der Kläger, ein klagebefugter Wettbewerbsverein, sah in einigen Inhalten der verlinkten Seite eine irreführende Werbung und damit einen Verstoß gegen die Vorschriften des Gesetzes gegen den unlauteren Wettbewerb (UWG). Der Kläger war der Auffassung, dass bereits mit der Verlinkung auf der Webseite des Orthopäden eine von ihm ausgehende Rechtsverletzung vorläge. Der Wettbewerbsverein mahnte den Orthopäden zunächst außergerichtlich ab und verlangte Unterlassung und Ersatz der angefallenen Anwaltskosten. Nachdem der Orthopäde sich weigerte, eine entsprechende Unterlassungserklärung zu unterzeichnen, erwirkte der Wettbewerbsverein gegen ihn eine einstweilige Verfügung auf Unterlassung beim zuständigen Landgericht. Das Oberlandesgericht (OLG) Köln sah anders als die Vorinstanz durch die Verlinkung auf die beanstandete Internetpräsenz keine Rechtsverletzung durch den Orthopäden als gegeben an und verneinte den vom Kläger geltend gemachten Anspruch auf Unterlassung und Ersatz der Abmahnkosten (siehe hierzu Klein in DFN-Infobrief Recht 07/2014, S. 5 ff.). Der BGH hat dieses Urteil des OLG Köln nun bestätigt.

Die Entscheidung des BGH

Der BGH lehnt, wie schon das OLG Köln, einen Unterlassungsanspruch nach den Vorschriften des UWG mit der Begründung ab, dass der beklagte Orthopäde nicht für die Inhalte der Webseite des Vereins einzustehen habe. Der BGH führt zu Beginn seiner Entscheidungsgründe noch einmal in die Gesetzeslage ein und betont, dass aufgrund fehlender konkreter Vorschriften im Hinblick auf die Haftung für Inhalte Dritter auf die allgemeinen Vorschriften abzustellen ist. Nach der bisher ergangenen höchstrichterlichen Rechtsprechung ist demnach maßgeblich, ob aus der objektiven Sicht eines verständigen Durchschnittsnutzers auf der Grundlage einer Gesamtbetrachtung aller Umstände sich der Webseitenbetreiber die verlink-

ten Inhalte zu Eigen gemacht hat. Anhand dieses Maßstabes ist nach Ansicht des BGH im konkreten Fall kein Zueigenmachen des Inhalts der Seite des Forschungsvereins durch die Verlinkung durch den Orthopäden gegeben. Das Gericht begründete seine Entscheidung damit, dass der Link auf dem Internetauftritt des Orthopäden weder einer Vervollständigung des eigenen Behandlungsangebotes diene, noch in einer Weise in einen redaktionellen Beitrag eingebettet sei, dass er für das „weitergehende Verständnis dort geäußelter Meinungen oder Ansichten erkennbar von Bedeutung und dadurch Bestandteil der vom Beklagten auf seiner Internetseite bereitgestellten Inhalte geworden ist“ (so der BGH hier mit Verweis auf BGH, Urteil v. 19. 5. 2011, Az.: I ZR 147/09). Auch wenn der BGH nicht weiter auf die Frage eingeht, bedeutet dies im Umkehrschluss, dass ein Zueigenmachen in den genannten Fällen durchaus anzunehmen ist. Der BGH würdigt ebenso wie die Vorinstanz als eines der maßgeblichen Kriterien, dass es sich bei dem bereitgestellten Link nicht um einen sog. Deeplink, also um einen Link, der unmittelbar auf konkrete Inhalte der verlinkten Webseite verweist, handelte. Vielmehr habe der Beklagte durch den Link lediglich auf die grundsätzlich unbedenkliche Startseite des beanstandeten Internetauftritts verwiesen und den Nutzer somit gerade nicht zu den wettbewerbsrechtlich in Frage stehenden Aussagen geführt. Nach Anklicken des Links ist es noch erforderlich, dass der Nutzer eine weitere vom Beklagten unabhängige Navigation auf dem Internetauftritt des Dritten vornimmt, um zu den beanstandeten Informationen zu gelangen. Das Gericht stützte demnach den vom Berufungsgericht gezogenen Vergleich, der hier empfehlende Link entspreche dem Hinweis auf weiterführende Literatur am Ende eines Aufsatzes oder Beitrages, über den sich der Nutzer zusätzliche Informationen zu einem bestimmten Thema selbstständig erschließen könne. Es sei fernliegend, dass der Verkehr die Verlinkung dahingehend verstehen könnte, der Beklagte wolle die inhaltliche Verantwortung für die Webseiteninhalte übernehmen.

Am Ende der Entscheidungsgründe geht der BGH auf die wettbewerbsrechtlichen Verkehrspflichten ein, die grundsätzlich eine Täterhaftung und damit einen Unterlassungsanspruch begründen können. Der BGH fordert hier gemäß seiner ständigen Rechtsprechung ein „gefährdendes Verhalten“, das sich grundsätzlich auch aus dem Setzen eines Hyperlinks ergeben kann, weil ein Hyperlink die Gefahr der Verbreitung des rechtswidrigen Inhalts des fremden Internetauftritts hervorrufen kann. Aus dieser Erhöhung der Gefahr einer Ver-

letzung wettbewerbsrechtlich geschützter Interessen folgt die Pflicht des Marktteilnehmers, die Gefahr im Rahmen des Möglichen und Zumutbaren zu begrenzen. Das Bestehen und der Umfang der Prüfpflichten bestimmen sich auch hier im Einzelfall nach einer Abwägung aller betroffenen Interessen und relevanten rechtlichen Wertungen. Der BGH nennt drei Anknüpfungspunkte, anhand derer sich der Umfang der auferlegten Prüfpflichten bemessen lässt. Zum einen kann auf den Gesamtzusammenhang, in dem der Hyperlink gesetzt wird, sowie auf dessen Zweck abgestellt werden. Darüber hinaus spielen die Kenntnis des Linksetzers über die Umstände, die darauf hinweisen, dass der verlinkte fremde Internetauftritt rechtswidrige Inhalte bereit hält, und die Möglichkeit des Erkennens solcher Inhalte eine entscheidende Rolle. Der BGH geht an dieser Stelle jedoch nicht weiter auf die einzelnen Anforderungen an die genannten Kriterien ein.

Eine Haftung könne sich aber zumindest für den Fall ergeben, in dem zunächst keine explizite Prüfpflicht besteht, der Hyperlink jedoch aufrecht erhalten bleibt, obwohl der Linksetzer z. B. durch eine Abmahnung oder Klageerhebung Kenntnis von einer möglichen Rechtswidrigkeit des Inhalts der verlinkten Seite erhalten hat. Aus dieser Kenntnis ergibt sich laut BGH dann eine zumutbare Prüfpflicht, an die jedoch in Fällen, in denen ein Hyperlink nur den Zugang zu allgemein zugänglichen Quellen erleichtern soll, im Interesse der Meinungs- und Pressefreiheit (Art. 5 Abs. 1 Grundgesetz) keine allzu strengen Anforderungen zu stellen sind. Der BGH verneint an dieser Stelle eine generelle proaktive Überwachungspflicht in Bezug auf die verlinkten Inhalte für den im Internet tätigen Unternehmer. Etwas anderes gelte aber, wenn der verlinkende Unternehmer von der Rechtswidrigkeit der verlinkten Inhalte Kenntnis erlangt. Im gegebenen Fall hat der beklagte Orthopäde nach Erhalt der Abmahnung den beanstandeten Link unverzüglich gelöscht, weshalb der BGH in diesem Falle keinen Pflichtenverstoß feststellen konnte. Am Ende der Entscheidung wird jedoch darüber hinausgehend betont, dass der Betreiber eines kommerziellen Internetauftritts aufgrund der wettbewerbsrechtlichen Interessen Dritter an dem Unterbleiben der Verbreitung rechtswidriger Inhalte im Internet sehr wohl eine Prüfpflicht haben kann. Dies sei insofern sachgerecht, als das Risiko der rechtlichen Beurteilung eines Links im Hinblick auf die Frage, ob die beanstandete Webseite des Dritten tatsächlich rechtswidrige Inhalte bereithält, demjenigen zuzuordnen sei, der den Link setzt. Das Privileg für spezielle Geschäftsmodelle wie File-Hosting-Dienste oder

Internetmarktplätze, bei denen eine Prüfpflicht grundsätzlich erst bei einer klaren Rechtsverletzung verlangt wird, könne nicht generell für Links auf kommerziellen Webseiten gelten, da eine Prüfpflicht bei einer begrenzten Anzahl von Links nach Ansicht des BGH zumutbar erscheint. Sobald der Unternehmer demnach einen Hinweis auf rechtswidrige Inhalte erhält, ist er verpflichtet, die Inhalte der verlinkten Webseite des Dritten zu prüfen. Dies gilt unabhängig davon, ob die Rechtsverletzung klar erkennbar ist oder nicht.

Fazit und Auswirkungen auf die Hochschulpraxis

Die Entscheidung des BGH lässt zunächst aufatmen. Es ist zu begrüßen, dass der BGH ein Zueigenmachen von Inhalten für die Fälle verneint, in denen ein Link lediglich zur unbeanspruchten Startseite eines fremden Internetauftritts führt, auch wenn dieser an anderer Stelle rechtsverletzende Inhalte aufweist. Allerdings kann die ergangene Entscheidung grundsätzlich nicht isoliert betrachtet werden, da die Frage, ob ein Zueigenmachen des fremden Inhalts gegeben ist, stets anhand des Einzelfalles zu bestimmen ist. Grundsätzlich ist für die Hochschulen zu beachten, dass es in Deutschland in der Vergangenheit auch Entscheidungen gab, in denen die höchstrichterliche Rechtsprechung Links kritischer gesehen und ein Zueigenmachen der verlinkten Inhalte in Einzelfällen bejaht hat. Demnach ist es wichtig, dass die Hochschulen ein Gespür dafür entwickeln, dass das Setzen eines Links unter Umständen rechtliche Konsequenzen nach sich ziehen könnte und immer anhand des jeweiligen Einzelfalles zu bewerten ist. Bereits kleine Unterschiede im Sachverhalt können zu einer abweichenden Bewertung führen. Im Idealfall sollten die Hochschulen davon Abstand nehmen, ohne weiteren Bedacht Links zu Internetauftritten Dritter zu setzen und es weitestgehend unterlassen, die Inhalte Dritter z. B. durch zustimmende Kommentare zu bewerten, sofern diese nicht offensichtlich rechtmäßig sind. Ein Disclaimer, der pauschal darauf hinweist, dass sich der Anbieter von den Inhalten Dritter distanziert, schadet grundsätzlich nicht, wirkt jedoch bei der Beurteilung, ob ein Zueigenmachen im konkreten Fall vorliegt, nur indiziell. Ein bedachter Einsatz eines Links, der einen objektiven Eindruck vermittelt und somit nicht auf eine Identifikation mit dem fremden Inhalt schließen lässt, sollte in den meisten Fällen unbedenklich sein. Es ist dennoch empfehlenswert, die verlinkte Seite stets genau in Augenschein zu nehmen und auf mögliche Rechtsverletzungen hin zu überprüfen, auch wenn

dies in Fällen wie dem hier dargestellten grundsätzlich nicht zwingend notwendig ist. Sollte ein sog. Deep-Link eingesetzt werden, der Link also nicht auf die Startseite eines Internetauftritts verweisen, sondern unmittelbar zu bestimmten rechtswidrigen Inhalten führen, kann hierin bereits – wie sich aus dem Umkehrschluss der Urteilsbegründung ergibt – ein Zueigenmachen des rechtswidrigen Inhalts gesehen werden, weshalb eine genaue Prüfung unbedingt erfolgen sollte.

Sobald die Hochschulen von Dritten auf mögliche Rechtsverletzungen durch die verlinkte Seite hingewiesen werden oder auf andere Weise Kenntnis von einer möglichen Rechtsverletzung erlangen, sollte der entsprechende Link unmittelbar entfernt werden, zumindest bis die rechtliche Unbedenklichkeit der Seite abschließend geklärt ist. Dieses Vorgehen beugt dem rechtlichen Risiko einer haftungsrechtlichen Inanspruchnahme vor.

Anmerkung:

Zur Entscheidung der Vorinstanz siehe Klein, „Das mach‘ ich doch mit Links!“, in: DFN-Infobrief Recht 07/2014

Privilegierte Störer?

Bundestag beschließt Gesetz zur Haftung von WLAN-Betreibern

von Lennart Sydow

Der Bundestag hat am 02.06.2016 mit dem „Zweiten Gesetz zur Änderung des Telemediengesetzes“ ein Gesetz verabschiedet, welches die Haftungsrisiken für WLAN-Betreiber beseitigen und dadurch zu einer größeren Verbreitung offener WLAN-Angebote führen soll. Darin werden zwar die WLAN-Betreiber ausdrücklich mit den schon bisher von einer Verantwortlichkeit für Rechtsverletzungen Dritter freigestellten Internet Providern gleichgestellt, die bei dieser Haftungsprivilegierung bestehende Rechtsunsicherheit kann aber dennoch nicht abschließend beseitigt werden.

I. Hintergrund und Gesetzgebungsverfahren

Die im Jahr 2007, in Umsetzung der Artikel 12-15 der E-Commerce-Richtlinie (RL 2000/31/EG), mit dem Telemediengesetz (TMG) eingeführten Haftungs Vorschriften der §§ 7–10 TMG beschäftigen seit Einführung regelmäßig die deutschen Gerichte. So wurde insbesondere in der Entscheidung „Sommer unseres Lebens“ des Bundesgerichtshofs (BGH) im Jahr 2010 die Haftung eines privaten WLAN-Betreibers für rechtswidrige Handlungen Dritter, die diese über einen nicht ausreichend gesicherten Internetanschluss begehen, festgestellt. Zwar werden in § 8 TMG die Access-Provider und in § 10 TMG die Host-Provider weitgehend von der Verantwortung für rechtsverletzende Inhalte Dritter, die sie speichern, übermitteln oder zu denen sie den Zugang vermitteln, freigestellt, solange sie eine rein passive Rolle einnehmen. Der BGH entschied aber, dass dies nicht für die Haftung auf Unterlassung der jeweiligen Tätigkeit im Rahmen der sogenannten Störerhaftung gelten sollte. Danach kann selbst derjenige, der nicht Täter oder Teilnehmer einer Rechtsverletzung ist, zur Unterlassung einer Handlung verpflichtet sein, wenn diese einen notwendigen Beitrag für die Rechtsverletzung darstellt. Als solcher Beitrag wurde vom BGH auch das Angebot eines nicht angemessen gesicherten WLAN angesehen. Dies führte bisher dazu, dass der Betrieb eines WLAN ohne ausreichende Zugangssicherung (z. B. durch WPA2 Passwortschutz) ein gewisses Haftungsrisiko für den Betreiber mit sich brachte (siehe aber für gewerbetreibende WLAN-Anbieter und zur Störerhaftung allgemein:

Overbeck, „Ich hab´s dir gesagt! Oder muss ich gar nicht?“ in: DFN-Infobrief Recht 08/2014).

Dieses Haftungsrisiko wurde von vielen Seiten stark kritisiert und unter anderem auch im Koalitionsvertrag 2013 als eine der Hauptursachen für die mangelnde Verbreitung offener WLAN-Angebote in Deutschland ausgemacht. Aus diesem Grund sollte durch eine Änderung des Telemediengesetzes Rechtssicherheit geschaffen und das Haftungsrisiko beseitigt werden. Nachdem ein erster Entwurf im März 2015 auf erhebliche Kritik gestoßen war, hatte die Bundesregierung im September 2015 einen überarbeiteten Entwurf des Bundesministeriums für Wirtschaft und Energie beschlossen und an den Bundestag weitergeleitet. Dort konnte man sich aber nach anhaltender Kritik von verschiedensten Parteien und Interessengruppen nicht darauf einigen, diesen zu verabschieden. Stattdessen wurde erst am 02.06.2016 ein erneut völlig überarbeiteter – und erheblich gekürzter – Gesetzesentwurf vom Bundestag beschlossen.

Mit den Stimmen der Regierungskoalition und gegen die der Oppositionsparteien hat der Bundestag nun das sogenannte „Zweite Gesetz zur Änderung des Telemediengesetzes“ beschlossen. Die darin enthaltenen Änderungen, zur Haftung von Access-Providern, beschränken sich allerdings auf die Hinzufügung eines Absatzes 3 in § 8 TMG, in dem die Haftungs-freistellung von Access-Providern geregelt ist. Anders als noch im Entwurf der Bundesregierung sieht § 8 TMG in seiner neu verabschiedeten Fassung keine besonderen Anforderungen für die Haftungsprivilegierung für WLAN-Anbieter vor, sondern

enthält lediglich die ausdrückliche Klarstellung, dass WLAN-Betreiber Diensteanbieter im Sinne des TMG sind und daher auch für sie die Haftungsprivilegierung des § 8 Abs. 1 TMG gilt.

II. Rechtliche Bedeutung der Gesetzesänderung

Die nun verabschiedete Änderung ist zwar insbesondere aus Sicht von Betreibern offener drahtloser Netzwerke zu begrüßen, kann aber nicht alle Zweifel an der vollständigen Haftungsfreistellung der Anbieter ausräumen.

Begrüßenswert ist sicherlich die erfolgte Gleichstellung der WLAN-Betreiber mit den klassischen Internet Providern. Dies stellt eindeutig klar, dass auch diese von der Haftungsprivilegierung des § 8 TMG profitieren und daher nicht für das Verhalten Dritter in ihrem Netz verantwortlich sind, solange sie lediglich die Durchleitung von Informationen vornehmen, also rein passiv tätig werden.

Nicht ausdrücklich durch die Änderung geklärt wird aber, ob diese Freistellung von der Verantwortlichkeit auch bedeutet, dass Unterlassungsansprüche gegenüber solchen Betreibern aufgrund der Störerhaftung ausgeschlossen sind. Zwar enthält die Gesetzesbegründung den Hinweis, diese Haftungsprivilegierung umfasse uneingeschränkt auch die verschuldensunabhängige Haftung im Zivilrecht nach der sogenannten Störerhaftung und stehe daher nicht nur einer Verurteilung des Vermittlers zur Zahlung von Schadenersatz, sondern auch seiner Verurteilung zur Tragung der Abmahnkosten und der gerichtlichen Kosten im Zusammenhang mit der von einem Dritten durch die Übermittlung von Informationen begangenen Rechtsverletzung entgegen. Allerdings ist dies eben nur in der Gesetzesbegründung und nicht im Gesetzestext enthalten und daher nicht zwingend bindend für die Gerichte. Es deckt sich zwar mit der Auslegung der zugrundeliegenden Richtlinie durch den Generalanwalt beim Europäischen Gerichtshof (EuGH), der dies in seinen Schlussanträgen vom 16. März 2016 in der Rechtssache C-484/14 ausführte. Problematisch könnte aber werden, dass der BGH mit zwei Urteilen vom 26.11.2015 (Az. I ZR 3/14 und I ZR 174/14) entschieden hat, dass Access-Provider verpflichtet sein können, Netzsperrn einzurichten, um den Zugang zu rechtswidrigen Inhalten zumindest zu erschweren und dies mit der Störerhaftung des Access-Providers begründet hat (s. hierzu Klein, „Den Letzten beißen die Hunde“ in: DFN-Infobrief Recht 04/2016). Diese beiden Ansichten scheinen miteinander nicht vereinbar, sodass

insgesamt unklar bleibt, ob die Störerhaftung nun durch die Haftungsprivilegierung des § 8 TMG ausnahmslos ausgeschlossen ist oder nicht.

Insgesamt wurde daher die Chance verpasst, endgültig Rechtssicherheit zu schaffen, auch wenn zu hoffen ist, dass die Rechtsprechung den Willen des Gesetzgebers aus der Gesetzesbegründung berücksichtigt und Abmahnungen diesbezüglich ohne Erfolg bleiben.

III. Auswirkungen für Hochschulen und Forschungseinrichtungen

Aus Sicht von Hochschulen und Forschungseinrichtungen sind die unmittelbaren Änderungen durch die Gesetzesänderung gering. Davon, dass sie in ihrer Funktion als Telekommunikationsdiensteanbieter gegenüber ihren Nutzern von der Haftungsprivilegierung des § 8 Abs. 1 TMG erfasst sind, konnte auch bisher ausgegangen werden. Der neu eingefügte Absatz 3 stellt diesbezüglich nur eine Klarstellung dar. Offene WLAN-Netze werden zudem von Hochschulen und Forschungseinrichtungen in der Regel nicht angeboten.

Die erhoffte Feststellung, dass auch Unterlassungsansprüche gegenüber Betreibern von Telekommunikationsnetzen und drahtlosen Netzwerken ausgeschlossen sind, enthält das Gesetz weiterhin nicht, sie kann lediglich aus der Gesetzesbegründung geschlossen werden.

Allerdings ist zumindest der ursprüngliche Entwurf der Bundesregierung, der Sicherungspflichten als Bedingung für die Haftungsprivilegierung privater Anbieter und darüber hinaus noch Verschärfungen für Host-Provider vorgesehen hatte, nun endgültig vom Tisch. Im Ergebnis gibt es daher zwar leider immer noch keine umfassende Rechtssicherheit, es besteht aber aufgrund dieser Gesetzesänderung für die Hochschulen und Forschungseinrichtungen auch kein Grund zur Sorge. Im Gegenteil scheinen auch Unterlassungsansprüche gegenüber Access-Providern in Zukunft noch unwahrscheinlicher, als dies bisher der Fall war. Rechtssicherheit könnte diesbezüglich möglicherweise das Urteil im angesprochenen Verfahren vor dem EuGH bringen.

Alles neu macht der Mai?!

Grundsätze für die Verarbeitung personenbezogener Daten nach der Datenschutz-Grundverordnung

von *Franziska Leinemann*

Mit der Geltung der Datenschutz-Grundverordnung (DS-GVO) ab Mai 2018 soll ein einheitliches Datenschutzniveau innerhalb der Europäischen Union gewährleistet werden. Datenverarbeiter müssen sich deshalb nun mit der Frage auseinandersetzen, welche Grundsätze die DS-GVO für die Verarbeitung personenbezogener Daten aufstellt. Um etwaige Neuerungen zu identifizieren, ist ein Vergleich mit der gegenwärtigen deutschen Rechtslage hilfreich.

I. Hintergrund

Nach jahrelangen Verhandlungen erzielten der Europäische Rat, das Europäische Parlament und die Europäische Kommission am 15. Dezember 2015 eine Einigung im Hinblick auf die DS-GVO. Diese bildet das Kernstück der Reform des Datenschutzrechts auf Ebene der Europäischen Union. Die DS-GVO wird nach einer zweijährigen Übergangsfrist am 25. Mai 2018 Geltung erlangen. Durch die Reform soll das Datenschutzrecht innerhalb der Europäischen Union weiter vereinheitlicht werden. Dies ist eines der Hauptziele. Die Verordnung hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat (Artikel 288 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union).

Der vorliegende Beitrag beschäftigt sich nun mit den Grundsätzen für die Verarbeitung personenbezogener Daten nach der DS-GVO. In Sydow, Vereinheitlichung des EU-Datenschutzrechts? – Die Datenschutz-Grundverordnung als anwendbares Recht für die DFN-Mitglieder, DFN-Infobrief Recht 05/2016, S. 2 ff. wurde im vergangenen Monat bereits das Verhältnis zum bisher geltenden Recht ausführlich beleuchtet. Auch Hintergründe und Ziele der Datenschutzreform auf Ebene der Europäischen Union sowie das Gesetzgebungsverfahren wurden erläutert.

II. Grundsätze

Die Grundsätze für die Verarbeitung personenbezogener Daten werden unter anderem in Artikel 5 DS-GVO benannt. Es kann bereits an dieser Stelle festgehalten werden, dass diese Grundsätze dem deutschen Recht nicht fremd sind. Vielmehr liegen sie auch den gegenwärtig anzuwendenden deutschen Datenschutzrechtsvorschriften zugrunde. Im Folgenden sollen die wichtigsten Grundsätze erläutert werden, auf denen die DS-GVO basiert und die somit tragende Bausteine des europäischen Datenschutzrechts sind. Es folgt jeweils ein Vergleich mit der aktuellen deutschen Gesetzeslage.

1. Verbot mit Erlaubnisvorbehalt

Zentrale Regel ist das Verbot mit Erlaubnisvorbehalt. Dies besagt, dass der Umgang mit personenbezogenen Daten grundsätzlich verboten ist. Er darf nur erfolgen, wenn er besonders legitimiert ist. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Artikel 4 Ziffer 1 DS-GVO), z. B. Namen, Anschrift, Geburtsdatum. Der Umgang mit personenbezogenen Daten ist beispielsweise dann erlaubt, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat oder die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (vgl. Artikel 5 Absatz 1 Buchstabe a), Artikel 6 DS-GVO).

Dieser Grundsatz liegt auch schon dem gegenwärtig anzuwendenden deutschen Datenschutzrecht zugrunde (vgl. § 4 Absatz 1 Bundesdatenschutzgesetz (BDSG), § 4 Absatz 1 Datenschutzgesetz NRW (DSG NRW)). An diesem grundlegenden Prinzip, das die Bedeutung des Rechts auf informationelle Selbstbestimmung widerspiegelt, ändert sich somit nichts.

2. Zweckbindung

Ein weiteres wichtiges Element ist die Zweckbindung. Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (Artikel 5 Absatz 1 Buchstabe b) DS-GVO). Erwähnenswert ist, dass unter anderem eine Weiterverarbeitung für wissenschaftliche oder statistische Zwecke von dieser Zweckbindung ausgenommen wird (Artikel 5 Absatz 1 Buchstabe b) DS-GVO). Abgesehen von diesen besonderen Fallgruppen stellt sich aber die Frage, wann eine Weiterverarbeitung für einen anderen Zweck möglich ist. Dies ist zunächst dann möglich, wenn eine Einwilligung vorliegt oder Rechtsvorschriften eingreifen, die eine Verarbeitung zu einem anderen Zweck erlauben. Ist dies nicht der Fall, bleibt letztlich nur eine Abwägung im Einzelfall (vgl. Artikel 6 Absatz 4 DS-GVO). Hier ist die Frage zu beantworten, ob die geplante Verarbeitung zu einem anderen Zweck mit demjenigen Zweck vereinbar ist, für den die Daten ursprünglich erhoben worden sind. Kriterien sind hier unter anderem jede Verbindung zwischen dem ursprünglichen Zweck und dem Zweck der beabsichtigten Weiterverarbeitung, der Zusammenhang, in dem die Daten erhoben wurden und die Art der personenbezogenen Daten (vgl. Artikel 6 Absatz 4 DS-GVO).

Die Zweckbindung ist auch tragender Baustein des gegenwärtigen deutschen Datenschutzrechts (vgl. zum Beispiel § 13 Absatz 1 DSG NRW). Eine Abweichung von der Zweckbindung ist nach aktueller Gesetzeslage jedoch nur im Rahmen eines abschließenden Katalogs an Fallkonstellationen möglich. Personenbezogene Daten dürfen nach geltendem Recht zum Beispiel dann zu Zwecken weiterverarbeitet werden, für die sie nicht erhoben worden sind, wenn Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen, oder es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder sonst einer unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Abwehr einer schwerwiegenden Beeinträchtigung

der Rechte einer anderen Person erforderlich ist (vgl. § 13 Absatz 2 DSG NRW). Aufgrund der allgemeinen Kriterien, die die DS-GVO aufstellt, liegt es nahe, von einer Aufweichung des Zweckbindungsgrundsatzes zu sprechen.

3. Transparenz

Des Weiteren beinhaltet die DS-GVO den Grundsatz der Transparenz (vgl. Artikel 5 Absatz 1 Buchstabe a) DS-GVO). Für betroffene Personen soll jeder Umgang mit sie betreffenden personenbezogenen Daten ersichtlich sein. Dies betrifft insbesondere die Erhebung und den Umfang der Verarbeitung der personenbezogenen Daten.

Der Grundsatz der Transparenz findet auch im BDSG und den Landesdatenschutzgesetzen Niederschlag, so zum Beispiel im Grundsatz der Direkterhebung und im Auskunftsrecht des Betroffenen. Der Grundsatz der Direkterhebung verlangt, dass personenbezogene Daten beim Betroffenen zu erheben sind (vgl. § 4 Absatz 2 Satz 1 BDSG).

4. Datenminimierung

Personenbezogene Daten müssen unter anderem dem Zweck angemessen sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden, sogenannte Datenminimierung (Artikel 5 Absatz 1 Buchstabe c) DS-GVO). In Artikel 25 DS-GVO wird der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen normiert. Dieser beinhaltet unter anderem die Aufforderung an den Verantwortlichen, geeignete technische und organisatorische Maßnahmen zu treffen, um die Datenschutzgrundsätze, wie zum Beispiel die Datenminimierung, wirksam umzusetzen. Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (Artikel 4 Ziffer 7 DS-GVO).

Für die aktuelle deutsche Rechtslage sei an dieser Stelle exemplarisch § 3a BDSG erwähnt. Dieser besagt, dass so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden sollen. Auch hier ist erneut die Nutzung technischer Möglichkeiten geboten.

5. Datensicherheit

Neben der Datenminimierung ist auch die Integrität und Vertraulichkeit personenbezogener Daten von grundlegender Bedeutung. Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet (Artikel 5 Absatz 1 Buchstabe f) DS-GVO). Erneut müssen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Artikel 32 Absatz 1 DS-GVO). Unter anderem kann und soll sich hier der Pseudonymisierung und Verschlüsselung personenbezogener Daten bedient werden. Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen sind (Artikel 4 Ziffer 5 DS-GVO).

Auch gegenwärtig haben Stellen, die Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten (vgl. § 9 BDSG). Gleiches gilt auf Landesebene (vgl. § 10 DSG NRW).

III. Fazit und Konsequenzen für die Hochschulpraxis

Die DS-GVO fußt auf jenen Grundprinzipien, die auch den gegenwärtig anzuwendenden deutschen Datenschutzrechtsvorschriften zugrunde liegen. Mit der Geltung der DS-GVO wird das Datenschutzrecht somit nicht auf den Kopf gestellt werden, vielmehr erscheinen bekannte Grundsätze und Regelungen vielfach lediglich in einem neuen Gewand. Der Mai 2018 macht nicht alles neu.

Verarbeiten Hochschulen personenbezogene Daten, gilt zunächst, dass sie als Verantwortliche den genannten Grundsätzen im Umgang mit personenbezogenen Daten gerecht

werden müssen. Besonderheiten können sich aufgrund der Existenz von Artikel 6 Absatz 2, Absatz 3 DS-GVO ergeben. Es handelt sich hierbei um eine sogenannte Öffnungsklausel (siehe hierzu vertiefend Sydow, Vereinheitlichung des EU-Datenschutzrechts? – Die Datenschutz-Grundverordnung als anwendbares Recht für die DFN-Mitglieder, DFN-Infobrief Recht 05/2016, S. 2 ff.). Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der DS-GVO in Bezug auf die Verarbeitung sowohl zur Erfüllung einer rechtlichen Verpflichtung als auch für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, beibehalten oder einführen. Hier bleibt das weitere Handeln des Gesetzgebers bis zur Geltung der DS-GVO ab Mai 2018 noch abzuwarten.

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

Nachdruck sowie Wiedergabe in elektronischer Form, auch auszugsweise, nur mit schriftlicher Genehmigung des DFN-Vereins und mit vollständiger Quellenangabe.