DFN

Infobrief Recht

6 / 2015

Juni 2015

Was lange währt… muss nicht immer gut sein

Rechtliche Probleme bei dem Angebot und der Nutzung einer automatischen E-Mail-Weiterleitung an Hochschulen

Die rechtlichen Herausforderungen von „Bring Your Own Device“ – Lifestyle contra Sicherheit

Teil 2: Arbeitsrecht, Urheberrecht

Ein Auskunftsverlangen, das man nicht ablehnen kann

Zum Auskunftsanspruch gegen Host-Provider bei Urheberrechtsverletzungen durch Dritte

Was lange währt… muss nicht immer gut sein

Rechtliche Probleme bei dem Angebot und der Nutzung einer automatischen E-Mail-Weiterleitung an Hochschulen

von Florian Klein

Die Nutzung einer automatischen E-Mail-Weiterleitung von der universitären E-Mail-Adresse auf eine private E-Mail-Adresse erfreut sich unter Hochschulmitgliedern seit Jahren großer Beliebtheit. Rechtlicher Risiken war man sich dabei meistens überhaupt nicht bewusst, sodass diese Praxis lange bedenkenlos Bestand hatte. Dass dieses Verhalten jedoch keineswegs ohne Weiteres rechtlich zulässig ist, soll in diesem Beitrag aufgezeigt werden, um Hochschulen zu animieren, die Aufrechterhaltung einer solchen Service-Option kritisch zu überdenken.

I. Hintergrund

Zu dem Service-Angebot einer Hochschule gehört es in aller Regel, dass Studierenden und Mitarbeitern ein eigener E-Mail-Dienst mit speziellen Hochschul-Mail-Adressen zur Verfügung gestellt wird, der über hochschuleigene Server betrieben wird. Einigen Hochschulmitgliedern ist die Nutzung eines solchen Dienstes jedoch zu unkomfortabel, weil sie bereits eine eigene private E-Mail-Adresse besitzen und ihre Kommunikation deshalb bevorzugt darüber abwickeln möchten. Um dies zu ermöglichen, bieten Hochschulen zusätzlich meist die Option an, im System eine private E-Mail-Adresse zu hinterlegen, auf die sämtliche E-Mails, die an die Hochschul-Mail-Adresse des jeweiligen Nutzers adressiert sind, automatisch weitergeleitet werden. Zum Teil kann dabei auch ausgewählt werden, ob im Hochschulpostfach zumindest eine Kopie der eingehenden und automatisch weitergeleiteten E-Mails abgelegt werden soll. Ist diese Einstellung einmal aktiviert, endet die Weiterleitung erst, wenn man diese manuell deaktiviert. Bis zu diesem Zeitpunkt werden alle E-Mails ohne jegliche menschliche Kontrolle des Inhalts an einen externen E-Mail-Provider weitergereicht, der dem Nutzer seine private E-Mail-Adresse zur Verfügung stellt. Dies kann in vielen Fällen dazu führen, dass kritische Informationen und Daten die Einflusssphäre der Hochschule verlassen und auf Servern landen, die keiner Kontrolle der Hochschule mehr unterliegen. Führt man sich dies vor Augen, drängen sich in Zeiten einer steigenden Bedeutung des Datenschutzes unweigerlich Zweifel auf, ob dies im Hinblick auf dienstliche Daten tatsächlich mit den geltenden Gesetzen vereinbar ist.

II. Rechtliche Betrachtung

Aus rechtlicher Sicht gibt es bei einer automatischen E-Mail-Weiterleitung in erster Linie vier Problemfelder: das Datenschutzrecht, den strafrechtlichen Geheimnisschutz, das Arbeitsrecht und das Informationsfreiheitsrecht. Vorab ist aber darauf hinzuweisen, dass viele rechtliche Fragen in diesem Zusammenhang kein Spezifikum der automatischen E-Mail-Weiterleitung sind, sondern sich durchaus auch bei einer manuellen, individuellen Weiterleitung stellen können. Eine Besonderheit ergibt sich allerdings aus der fehlenden inhaltlichen Kontrollmöglichkeit bei einer automatischen E-Mail-Weiterleitung, da diese sich ja gerade dadurch auszeichnet, dass jede Mail unterschiedslos weitergeleitet wird. Kann im Einzelfall deshalb überhaupt nicht festgestellt werden, welche Daten und Inhalte weitergeleitet werden, ist für die Beurteilung der rechtlichen Zulässigkeit im Zweifel davon auszugehen, dass darunter auch kritische Inhalte sind, für deren Weitergabe spezielle rechtliche Anforderungen bestehen, zumal

E-Mails sehr häufig Daten beinhalten, die dem Datenschutzrecht unterliegen.

Um den verschiedenen rechtlichen Fragen in hinreichendem Maße gerecht werden zu können, befasst sich dieser Beitrag zunächst nur mit dem Datenschutzrecht. Im kommenden Monat folgt dann der zweite Teil, der sich mit den übrigen drei Rechtsgebieten auseinandersetzt.

1. Rechtliche Beurteilung bei Mitarbeitern

Hochschulen sind in vielen Fällen als Körperschaften des öffentlichen Rechts organisiert. In Nordrhein-Westfalen legt dies beispielsweise § 2 Abs. 1 S. 1 Hochschulgesetz NRW (HG NRW) fest. Insofern ergibt sich, dass die jeweiligen Landesdatenschutzgesetze für staatliche Hochschulen als öffentliche Stellen zur Anwendung kommen und Datenverarbeitungen der Hochschulen deshalb an deren Maßstab zu messen sind. Da jedes Bundesland ein eigenes Landesdatenschutzgesetz erlassen hat, erfolgt die Darstellung hier exemplarisch anhand des nordrhein-westfälischen Datenschutzgesetzes. Die meisten Ausführungen lassen sich jedoch auf die anderen Bundesländer übertragen, da die wesentlichen Grundsätze in allen Bundesländern sehr ähnlich sind.

Die erste Differenzierung, die bei der rechtlichen Betrachtung vorzunehmen ist, ist die zwischen Mitarbeitern der Hochschule und Studierenden, da insofern unterschiedliche Regelungen zu beachten sind. Mitarbeiter sind Teil der Hochschule und ihr Verhalten wird dieser zugerechnet, soweit sie zur Erfüllung ihrer Aufgaben tätig werden und in einem Arbeits- bzw. Beamtenverhältnis zu ihr stehen. Insofern ergeben sich aus dem Status als Beamter oder Angestellter im öffentlichen Dienst keine Unterschiede. Dienstliche Tätigkeiten der Mitarbeiter werden somit nach dem für die Hochschule geltenden Datenschutzrecht beurteilt, wobei die Hochschule nach außen die für diese Datenverarbeitungen verantwortliche Stelle ist.

Relevante Datenverarbeitung

Ausgangspunkt jeder datenschutzrechtlichen Betrachtung ist die Feststellung, ob personenbezogene Daten in einer Weise verarbeitet werden, die vom Datenschutzgesetz erfasst ist. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 DSG NRW). In Bezug auf die Daten, die typischerweise in einer E-Mail enthalten sind, sind dies beispielsweise (personalisierte) E-Mail-Adressen, Namen, Kontaktdaten und Ähnliches. Werden also E-Mails automatisch an eine andere Adresse weitergeleitet, sind in aller Regel auch personenbezogene Daten betroffen.

Problematisch ist dies dann, wenn in der Weiterleitung der E-Mails eine Datenverarbeitung zu sehen ist. Zu denken ist vorrangig an eine Datenübermittlung. Als Übermitteln definiert das Gesetz das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die verantwortliche Stelle weitergegeben oder zur Einsichtnahme bereitgehalten werden […]. Dabei soll eine Übermittlung nicht nur dann vorliegen, wenn der Empfänger die personenbezogenen Daten tatsächlich zur Kenntnis nimmt, sondern auch schon dann, wenn er nur die faktische Möglichkeit hat, die Daten tatsächlich zur Kenntnis zu nehmen. Warum diesem Übermittlungsbegriff ein derart weites Verständnis zugrunde gelegt wird, erschließt sich bei einem Blick auf den Sinn und Zweck der Regelungen zur Datenübermittlung: es geht nämlich primär darum, jegliche gezielte Ausweitung des Personenkreises, dem die personenbezogenen Daten zugänglich sind, zu verhindern und eine solche droht schon dann, wenn nur die faktische Möglichkeit der Kenntnisnahme besteht.

Dritter ist im Fall der automatischen E-Mail-Weiterleitung, bei der ein Mitarbeiter seine eingehenden E-Mails an eine private E-Mail-Adresse weiterleiten lässt, nicht der Mitarbeiter als Inhaber der E-Mail-Adresse, sondern dessen Mail-Provider. Sofern es nicht um hochschulinterne Weiterleitungen geht, bei denen diese Problematik nicht besteht, ist der Anbieter des Mailing-Dienstes weder Teil der Hochschule noch steht er in einem besonderen Verhältnis zu ihr, sodass er sich außerhalb der verantwortlichen Stelle befindet.

Damit eine datenschutzrechtlich relevante Übermittlung vorliegt, müssten die jeweiligen Daten also auch durch die Hochschule an den Mail-Provider weitergegeben werden. Der Begriff der Weitergabe erfasst jede Handlung, durch die die in den Daten enthaltenen Informationen in den Bereich des Empfängers gelangen. Auch wenn der Zweck der E-Mail-Weiterleitung nicht darin liegt, seinem privaten E-Mail-Provider Informationen zu verschaffen, gelangen dadurch die Daten aus allen dienstlichen E-Mails in dessen Machtbereich und können theoretisch von diesem eingesehen werden, solange

die Inhalte nicht verschlüsselt sind. Schon auf dem Transportweg werden E-Mails häufig mit Postkarten verglichen, da sie leicht abgefangen und die Inhalte ausgelesen werden können. Sind sie aber erst auf dem fremden Mail-Server eingegangen, kann der Mail-Provider erst recht faktisch ohne Probleme auf sie zugreifen.

Selbst wenn zum Teil gefordert wird, dass eine tatsächliche Kenntnisnahme der Daten durch den Dritten erfolgt, ist eine solche Kenntnisnahme nicht immer auszuschließen, da beispielsweise Anbieter wie Google tatsächlich E-Mail-Inhalte scannen und – mindestens zu Werbezwecken – automatisiert auswerten. Als Gegenpol dazu stehen unter anderem die deutschen Anbieter, die an das Fernmeldegeheimnis gebunden sind und die deshalb nicht auf die E-Mail-Inhalte zugreifen dürfen. Dies schließt einen Zugriff allerdings nur rechtlich und keineswegs faktisch aus. Auch diese haben also die tatsächliche Möglichkeit einer Kenntnisnahme, sodass im Zweifel selbst bei diesen eine Weitergabe zu bejahen sein dürfte.

Dass diese Weitergabe auch durch die Hochschule als verantwortliche Stelle erfolgt, ergibt sich daraus, dass der jeweilige Hochschulmitarbeiter die automatische E-Mail-Weiterleitung aktiviert und damit die Weitergabe der Daten sämtlicher eingehender E-Mails veranlasst hat. Dieses Verhalten muss sich die Hochschule zurechnen lassen. Es ist allerdings darauf hinzuweisen, dass diese Konstellation einer automatischen E-Mail-Weiterleitung in der Rechtswissenschaft bisher kaum diskutiert wurde.

Dennoch lässt sich als weiteres Argument für die Einordnung als Datenübermittlung eine Parallele zum Cloud-Computing anführen. Zwar gibt es dieses in verschiedensten Ausprägungen, doch ist eine davon die Bereitstellung von Speicherplatz auf Servern des externen Diensteanbieters für den Cloud-Nutzer. Nimmt jemand einen solchen Dienst in Anspruch und verlagert seine Daten in den Cloud-Speicher, erfolgt dies nicht mit der Intention, dass der Cloud-Anbieter diese zur Kenntnis nehmen soll, sondern dient vorwiegend der Arbeitserleichterung, da die Daten von überall über das Internet abrufbar sind und man sich das Vorhalten eigener großer Speichermedien ersparen kann. Dennoch ist der Cloud-Anbieter faktisch in der Lage, die gespeicherten Daten zur Kenntnis zu nehmen. Hier besteht also eine Konstellation, die der E-Mail-Weiterleitung sehr ähnlich ist, da in beiden Fällen externe Diensteanbieter faktisch Zugriffsmöglichkeiten auf fremde Daten erhalten, auch wenn die Ausnutzung dieser Zugriffsmöglichkeiten vom Nutzer nicht gewollt ist.
Im Hinblick auf das Cloud-Computing mithilfe externer Diensteanbieter besteht weitgehend Einigkeit, dass dieses als sogenannte Auftragsdatenverarbeitung zu qualifizieren ist. Die Auftragsdatenverarbeitung (§ 11 DSG NRW) ist ein rechtliches Konstrukt, das es datenverarbeitenden Stellen erleichtern soll, sich bei der Datenverarbeitung der Unterstützung externer Stellen zu bedienen. Das funktioniert dadurch, dass das Gesetz einen externen Datenverarbeiter nicht als Dritten ansieht, wenn eine wirksame Vereinbarung über die Auftragsdatenverarbeitung geschlossen wurde. Dies führt dazu, dass eine Weitergabe von Daten an ihn im Rechtssinne keine Übermittlung von Daten darstellt und deshalb unter erleichterten Voraussetzungen zulässig ist. Verantwortlich bleibt bei dieser Konstruktion stets der Auftraggeber, der verpflichtet ist, sich im Rahmen der Vereinbarung Kontroll- und Weisungsrechte von dem externen Dienstleister einräumen zu lassen und die Umstände der Datenverarbeitung zu regeln.

Zugleich bedeutet dies aber auch, dass bei einer unwirksamen oder einer nicht vorhandenen Vereinbarung über die Durchführung einer Auftragsdatenverarbeitung die gesetzliche Privilegierung der Datenweitergabe nicht eingreifen kann und dann eine Datenübermittlung vorliegen muss. Denn wenn die Weitergabe der Daten an den Cloud-Anbieter als solche keine Datenübermittlung im Sinne des Datenschutzgesetzes darstellen würde, bräuchte man gar keine Auftragsdatenverarbeitung. Nimmt man also diese Parallele des Cloud-Computings zu Hilfe, ergibt sich auch für die automatische E-Mail-Weiterleitung, dass in der Weiterleitung der E-Mails an eine private E-Mail-Adresse eine Übermittlung der darin enthaltenen Daten an den E-Mail-Provider zu sehen ist.

Doch selbst wenn man dies ungeachtet der oben stehenden Argumente bestreiten möchte, verbleibt immer noch eine datenschutzrechtlich relevante Nutzung von Daten (§ 3 Abs. 2 Nr. 7 DSG NRW), da dies als Auffangtatbestand jede sonstige Verwendung personenbezogener Daten erfasst.

Datenschutzrechtliche Erlaubnistatbestände

Ist also das Vorliegen einer datenschutzrechtlich relevanten Verwendung festgestellt, ist für deren Zulässigkeit erforderlich, dass eine Einwilligung des Betroffenen vorliegt oder eine gesetzliche Vorschrift dieses Verhalten erlaubt (§ 4 DSG NRW).

Von einer Einwilligung des Betroffenen wird man bei einer automatischen E-Mail-Weiterleitung indes nicht ohne Weiteres ausgehen können. Zum einen weiß der Absender überhaupt nicht, dass seine E-Mails, die er an eine Hochschuladresse sendet, an einen anderen Mail-Provider weitergeleitet werden und muss damit auch nicht zwingend rechnen, sodass allein der Versand einer E-Mail, die personenbezogene Daten enthält, noch nicht als Einwilligung durch schlüssiges Verhalten eingestuft werden kann. Zum anderen könnte der Absender ohnehin nur in die Verwendung der eigenen Daten einwilligen. Im Hinblick auf die Daten Dritter, die potentiell per E-Mail verschickt werden, wäre die Einwilligung des jeweiligen Dritten erforderlich, die naturgemäß nicht vom Absender der E-Mail erteilt werden kann.

Dass das DSG NRW oder eine andere Rechtsvorschrift eine solche Datenverwendung erlaubt, kann ebenfalls nicht pauschal unterstellt werden. Insbesondere ist nicht ersichtlich, inwiefern eine automatische E-Mail-Weiterleitung zur Aufgabenerfüllung der Hochschule erforderlich ist, da in aller Regel auch mit den Hochschul-Mail-Adressen gearbeitet werden kann und ein potentiell geringfügig verringerter Komfort gegenüber privaten Mail-Adressen nicht ausreichend ist, um die strengen Anforderungen des Erforderlichkeitskriteriums zu erfüllen. Da also keineswegs für alle Fälle sichergestellt ist, dass ein Erlaubnistatbestand eingreift, bestehen nicht unerhebliche datenschutzrechtliche Bedenken gegenüber einer automatischen E-Mail-Weiterleitung.

Dies gilt umso mehr, als bei Datenübermittlungen an E-Mail-Provider, die ihren Sitz außerhalb der EU-Mitgliedstaaten haben, wie dies z.B. bei den US-amerikanischen Anbietern der Fall ist, noch höhere Anforderungen gelten. So muss im Normalfall nämlich, zusätzlich zu den üblichen Zulässigkeitsvoraussetzungen, ein angemessenes Datenschutzniveau gewährleistet werden (§ 17 DSG NRW), welches in den meisten Fällen nicht vorliegt und nur durch besondere Vorkehrungen geschaffen werden kann (z.B. durch die Vereinbarung sogenannter Standardvertragsklauseln).

Datenschutz durch technische und organisatorische Maßnahmen

Außerdem ist zu berücksichtigen, dass die Landesdatenschutzgesetze die verantwortlichen Stellen dazu verpflichten, die Ausführung und Einhaltung der datenschutzrechtlichen Vorschriften durch technische und organisatorische Maßnahmen sicherzustellen (z.B. § 10 DSG NRW). Zur Konkretisierung dieser Verpflichtung enthalten die Gesetze eine Auflistung bestimmter Maßnahmen, die der Gewährleistung verschiedener datenschutzrechtlicher Schutzstandards dienen sollen. Dazu gehört beispielsweise, dass die Vertraulichkeit und Verfügbarkeit der Daten sichergestellt werden müssen, indem Maßnahmen getroffen werden, die garantieren, dass die Daten nur von Befugten zur Kenntnis genommen werden können, zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.

Bei der Nutzung einer automatischen E-Mail-Weiterleitung gelangen geschützte Daten in die Hände eines Dritten, bei dem nicht sichergestellt ist, dass er seinerseits die erforderlichen Schutzmaßnahmen getroffen hat. Dazu kommt, dass die Hochschulen auf die externen Mail-Provider überhaupt keinen Einfluss und deshalb keine Kontroll- oder Steuerungsmöglichkeit zur Einführung der erforderlichen technischen und organisatorischen Maßnahmen haben. Darüber hinaus dürfte man zu den erforderlichen organisatorischen Maßnahmen der Hochschule in einem solchen Fall zählen können, dass sie ihren Mitarbeitern untersagt, solche automatischen E-Mail-Weiterleitungen einzurichten und dies auch technisch verhindert oder zumindest erschwert, indem entsprechende Funktionen gar nicht erst angeboten werden. Die allgemeine Pflicht der Hochschule, ihren Betrieb so zu organisieren, dass geltende Gesetze Beachtung finden und möglichst keine Rechtsverletzungen begangen werden („Compliance“), ist hier im Hinblick auf den Datenschutz spezialgesetzlich konkretisiert. Das Service-Angebot einer automatischen E-Mail-Weiterleitung für dienstliche E-Mail-Konten, welches sich technisch relativ leicht verhindern lässt, wird man deshalb als Verstoß gegen § 10 DSG NRW ansehen müssen.

Pflichten gegenüber der Datenschutzaufsicht

Problematisch ist die automatische E-Mail-Weiterleitung zudem im Hinblick auf die Verpflichtungen, die der Hochschule gegenüber der Datenschutzaufsicht obliegen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI) hat eine Aufsichtsfunktion gegenüber den öffentlichen Stellen, da das Gesetz vorsieht, dass er die Einhaltung der datenschutzrechtlichen Vorschriften bei diesen überwacht (§ 22 DSG NRW). Um diese Aufgabe erfüllen zu können, sind die Hochschulen als öffentliche Stellen generell verpflichtet, den LDI bei seiner

Aufgabe zu unterstützen und erforderlichenfalls Amtshilfe zu leisten. Insbesondere sind ihm Auskünfte über Fragen zur Datenverarbeitung zu erteilen, Einsicht in alle Datenverarbeitungsvorgänge, Dokumentationen und Aufzeichnungen zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, jederzeit Zutritt zu allen Diensträumen und Zugriff auf elektronische Dienste zu ermöglichen und ggf. auch Kopien von Unterlagen zur Verfügung zu stellen. Im Einzelfall kann dies auch bedeuten, dass bestimmte dienstliche E-Mails vorzulegen sind. Wenn nun aber die E-Mails nur noch in privaten Postfächern auf fremden Servern liegen, weil sie ohne Speicherung einer Kopie im Postfach der Hochschul-Mail-Adresse automatisch weitergeleitet werden, ist der Hochschule die Erfüllung dieser Verpflichtung faktisch oft nicht mehr möglich. Dieses Problem stellt sich in ähnlicher Hinsicht auch noch unter zwei anderen rechtlichen Aspekten (Arbeitsrecht und Informationsfreiheitsrecht), die allerdings erst im zweiten Teil dieses Beitrags dargelegt werden.

Löschungspflichten

Zu guter Letzt ist noch zu bedenken, dass das Datenschutzrecht Löschungspflichten in Bezug auf solche personenbezogenen Daten vorsieht, deren Speicherung unzulässig ist oder deren Kenntnis nicht mehr zur Aufgabenerfüllung der verarbeitenden Stelle erforderlich ist. Dies ist Ausfluss des Grundsatzes der Datensparsamkeit und der Datenvermeidung, wonach möglichst wenige personenbezogene Daten erhoben und verarbeitet werden sollen und dies auch nur solange wie nötig. Die Einhaltung dieser Löschungspflichten kann nicht mehr effektiv durch die Hochschule kontrolliert werden, wenn die E-Mails mit entsprechenden Daten nicht mehr in ihrem Einflussbereich gespeichert sind, sondern auf den Servern externer Mail-Provider liegen.

Rechtsfolgen

Für datenschutzrechtliche Verstöße bestehen in verschiedenem Maße gesetzliche Sanktionen. So erklärt § 34 DSG NRW die rechtswidrige Weitergabe nicht offenkundiger personenbezogener Daten zur Ordnungswidrigkeit, die mit einer Geldbuße bis zu 50.000 € geahndet werden kann. Diese ordnungsrechtliche Verantwortlichkeit ist zuvorderst eine persönliche und trifft deshalb denjenigen Mitarbeiter, der die automatische E-Mail-Weiterleitung eingestellt und genutzt hat. Im Einzelfall kann jedoch unter den hier nicht näher zu erörternden Voraussetzungen des § 30 Ordnungswidrigkeitengesetz (OWiG) auch eine Geldbuße gegen die Hochschule verhängt werden. Dies kann relevant werden, wenn der Leitungsebene eine Aufsichtspflichtverletzung dergestalt vorzuwerfen ist, dass unzureichende organisatorische Vorkehrungen zur Sicherstellung der Einhaltung datenschutzrechtlicher Regelungen getroffen wurden.

Darüber hinaus kann jeglicher Verstoß gegen datenschutzrechtliche Vorschriften gemäß § 24 DSG NRW zu einer Beanstandung durch den LDI führen, der insofern eine Aufsichtsaufgabe hat. Eine solche Beanstandung müsste gegenüber dem Rektor erfolgen und ist mit einer Aufforderung zur Abgabe einer Stellungnahme verbunden, welcher innerhalb einer bestimmten Frist nachgekommen werden muss. Gleichzeitig unterrichtet der LDI auch die Aufsichtsbehörde. Dies ist unter anderem deshalb notwendig, weil der LDI selbst – zumindest in einigen Bundesländern – keine Durchsetzungsbefugnisse hat. Verweigert die Hochschule trotz Beanstandung durch den LDI eine Anpassung des Verhaltens und teilt die Aufsichtsbehörde die Ansicht des LDI, kann diese (im Fall der nordrhein-westfälischen Hochschulen ist dies das Ministerium für Innovation, Wissenschaft und Forschung des Landes Nordrhein-Westfalen) dann gegebenenfalls die Durchsetzung erzwingen. Im Hinblick auf die konkrete Vorgehensweise in anderen Bundesländern ist auf die entsprechenden Normen der jeweiligen Landesdatenschutzgesetze zu verweisen.

Schließlich ist noch zu beachten, dass § 20 DSG NRW einen Schadensersatzanspruch des Betroffenen vorsieht, wenn dieser einen Schaden durch eine unrichtige oder unzulässige Datenverarbeitung erleidet. In schweren Fällen kann der Betroffene sogar einen Anspruch auf Ersatz seiner immateriellen Schäden haben („Schmerzensgeld“). Das erforderliche Verschulden der verantwortlichen Stelle wird dabei vermutet, kann aber widerlegt werden, sofern es tatsächlich an einem fahrlässigen oder vorsätzlichen Handeln fehlte. Erfolgte die Datenverarbeitung in einer automatisierten Datei, ist der Schadensersatzanspruch sogar verschuldensunabhängig, dafür allerdings in der Höhe auf einen bestimmten Betrag gedeckelt. Anspruchsgegner ist insofern in jedem Fall die Hochschule als Träger der verantwortlichen Stelle.

2. Rechtliche Beurteilung für Studierende

Für Studierende sind gesonderte Erwägungen anzustellen. Selbst wenn diese nach dem jeweiligen Hochschulgesetz als

Mitglieder der Hochschule qualifiziert werden (so z.B. für eingeschriebene Studierende § 9 Abs. 1 S. 1 HG NRW) und damit in einem Sonderrechtsverhältnis zur Hochschule stehen, muss die Hochschule sich deren Verhalten nicht ohne Weiteres zurechnen lassen. Sie sind deshalb datenschutzrechtlich nicht Teil der öffentlichen Stelle „Hochschule", sodass ihr Handeln auch nicht nach dem Landesdatenschutzgesetz zu beurteilen ist. Vielmehr unterliegen sie als Private dem Bundesdatenschutzgesetz (BDSG) und sind dessen Terminologie folgend sogenannte „nicht-öffentliche Stellen". Das BDSG wiederum legt in § 1 Abs. 2 Nr. 3 fest, dass es dann nicht anwendbar ist, wenn solche nicht-öffentlichen Stellen eine Datenverarbeitung ausschließlich für persönliche oder familiäre Tätigkeiten vornehmen. Hiermit will der Gesetzgeber Privatleute in einem engen Kreis von den Restriktionen des Datenschutzrechts befreien, um ihr privates Handeln nicht unverhältnismäßig zu erschweren. Zu diesem engen persönlichen Bereich sollen auch Tätigkeiten im Rahmen der Aus- und Fortbildung gehören, wozu man auch das Studium zählen können wird, solange die jeweiligen Tätigkeiten nicht über den üblichen persönlichen Kreis hinausreichen. Richten sich Studierende also eine automatische E-Mail-Weiterleitung von ihrer Hochschul-Mail-Adresse auf eine private E-Mail-Adresse ein und nutzen diese für Zwecke des Studiums und andere private Angelegenheiten, sind die Voraussetzungen dieses speziellen Anwendungsbereichsausschlusses erfüllt und das Datenschutzrecht deshalb nicht anwendbar. Daraus folgt zugleich, dass insoweit anders als bei den Mitarbeitern datenschutzrechtliche Bedenken nicht bestehen und zahlreiche Fälle denkbar sind, in denen die Nutzung einer automatischen E-Mail-Weiterleitung durch Studierende rechtmäßig möglich ist.

Dieser Rahmen einer Datenverarbeitung zu ausschließlich persönlichen Zwecken wird jedoch überschritten, sobald Studierende bestimmte Selbstverwaltungsaufgaben der Hochschule wahrnehmen, indem sie beispielsweise in Gremien, Ausschüssen, Fachschaften oder Ähnlichem tätig werden und dabei personenbezogene Daten verarbeiten. Insoweit kommt das Datenschutzrecht also auch für Studierende zur Anwendung. Das Gleiche gilt für eine sonstige Nutzung der E-Mail-Adresse für Tätigkeiten, die über den persönlichen Bereich hinausgehen. Obwohl dies keine seltenen Konstellationen sind, dürfte es unverhältnismäßig sein, allein deshalb ein pauschales Verbot des Angebots einer automatischen E-Mail-Weiterleitung für alle Studierenden zu fordern. Stattdessen rückt hier die Eigenverantwortung der jeweiligen Studierenden in den Vordergrund, die zunächst selbst dafür Sorge tragen müssen, dass sie gesetzeskonform handeln. Aufgrund der allgemeinen Pflicht der Hochschule zur Organisation des Hochschulbetriebs in der Form, dass gesetzliche Verbote eingehalten werden und insbesondere auch das Datenschutzrecht Beachtung findet, könnte man von ihr aber unter Umständen verlangen, dass sie Studierende, die in Hochschulgremien tätig sind, darauf hinweist, dass die Nutzung einer automatischen E-Mail-Weiterleitung datenschutzrechtlich nicht risikolos und potentiell rechtswidrig ist. Deshalb bietet es sich an, im Rahmen des Aktivierungsprozesses der automatischen E-Mail-Weiterleitung für Studierende einen entsprechenden Warnhinweis aufzunehmen, dessen Kenntnisnahme bestätigt werden muss, sofern dieses Service-Angebot für Studierende überhaupt aufrechterhalten werden soll.

Darüber hinaus verpflichtet § 11 Abs. 3 HG NRW die Mitglieder der Hochschule ohnehin in allen Angelegenheiten zur Verschwiegenheit, die ihnen als Träger eines Amtes oder einer Funktion bekannt geworden sind und deren Vertraulichkeit sich aus Rechtsvorschriften, auf Grund besonderer Beschlussfassung des zuständigen Gremiums oder aus der Natur des Gegenstandes ergibt. Verstöße gegen diese Verschwiegenheitspflicht können durch Maßnahmen zur Wiederherstellung der Ordnung geahndet werden, welche allerdings von der Hochschule entsprechend geregelt sein müssen (§ 11 Abs. 5 HG NRW). Ob diese Verschwiegenheitspflicht bei der Nutzung einer automatischen E-Mail-Weiterleitung eingehalten wird, bei der potentiell solche geheimen Inhalte in den Machtbereich des externen E-Mail-Providers gelangen, ist zumindest zweifelhaft.

III. Fazit

Schon die datenschutzrechtliche Betrachtung hat gezeigt, dass das Service-Angebot einer automatischen E-Mail-Weiterleitung durch Hochschulen jedenfalls für ihre Mitarbeiter rechtliche Risiken mit sich bringt, denen nur durch die Abschaffung dieses Angebots sicher vorgebeugt werden kann. Festzuhalten sind aber auch zwei andere Fakten: zum einen stellen sich diese Probleme in der Regel nicht bei Weiterleitungen an eine andere hochschulinterne E-Mail-Adresse desselben Nutzers, da der Herrschaftsbereich der verantwortlichen Stelle dabei nicht verlassen wird und die Daten nicht in die Hände eines Dritten gelangen. Zum anderen ist darauf hinzuweisen, dass bisher – soweit ersichtlich – weder Gerichtsentscheidun-

gen zu dieser Fragestellung ergangen sind noch sonstige Fälle einer Ahndung eines solchen Angebots bekannt geworden sind. Auch die rechtswissenschaftliche Literatur setzt sich so gut wie gar nicht mit diesem Problem auseinander. Ganz vereinzelt finden sich jedoch ebenfalls kritische Einschätzungen. Dennoch ist zu berücksichtigen, dass die Sensibilität für datenschutzrechtliche Fragestellungen und Standards angesichts fortwährender Diskussionen über Vorratsdatenspeicherung und scheinbar allgegenwärtige Überwachung durch Geheimdienste in der Bevölkerung zunimmt. Ferner sind öffentliche Stellen schon durch das Grundgesetz an Gesetz und Recht gebunden und haben eine gewisse Vorbildfunktion. Insofern sollte es nicht zum Maßstab des Handelns gemacht werden, dass dieses Angebot teils schon jahrelang Bestand hatte, ohne dass es Beanstandungen gab. Generell rechtfertigt eine lange Ausübung eines rechtswidrigen Verhaltens keine Fortführung dieser Zustände in der Zukunft. Vielmehr gehört die automatische E-Mail-Weiterleitung auf den Prüfstand der Hochschulen.

Für Studierende dagegen dürfte die automatische E-Mail-Weiterleitung aus datenschutzrechtlicher Perspektive in der Regel deutlich weniger kritisch einzustufen sein. Soweit einige Studierende im Rahmen der Aufgabenerfüllung der Hochschule in Gremien tätig werden und insoweit auch an das Datenschutzrecht gebunden sind, dürfte es unter dem Blickwinkel der Verhältnismäßigkeit vertretbar sein, dieses Service-Angebot für Studierende nicht generell abzuschaffen, sondern dessen Inanspruchnahme nur mit einer Aufklärung und einem entsprechenden Warnhinweis zu versehen. Denn es verbleibt immer noch ein großer Kreis von Studierenden, für die eine Nutzung der automatischen E-Mail-Weiterleitung datenschutzrechtlich zulässig sein dürfte.

Die rechtlichen Herausforderungen von „Bring Your Own Device“ – Lifestyle contra Sicherheit

Teil 2: Arbeitsrecht, Urheberrecht

von Kevin Kuta

Die Rechenleistung und Komplexität mobiler Endgeräte ist in den letzten Jahren derart gestiegen, dass sie mit herkömmlichen PCs mithalten oder diese sogar leistungstechnisch übersteigen. Überall und jederzeit ist damit der Zugriff auf lokale Anwendungen und Daten möglich, meist auch mit einer direkten Verbindung zum Internet. Gleichzeitig bieten die Cloud-Technologien einen nahezu unbegrenzten Zugang auf global gespeicherte Daten über diese Geräte. Neben der Wirtschaft hat auch die öffentliche Verwaltung die vielfältigen und flexiblen Möglichkeiten dieser Geräte für sich entdeckt. Mitarbeitern ist eine gewohnte und einfache Arbeitsumgebung sehr wichtig. Nirgends können sie derartige Umstände besser vorfinden als auf ihren eigenen Endgeräten. Es stellt sich daher die Frage, welche rechtlichen Probleme bei der Nutzung privater Endgeräte zu dienstlichen Zwecken („Bring Your Own Device“, kurz „BYOD“) bestehen.
Bei diesem Beitrag handelt es sich um die Fortsetzung der im DFN-Infobrief Recht Ausgabe 04/2015 begonnenen Reihe zum Thema „Bring Your Own Device“ („BYOD“). In dieser Ausgabe wird dieses Konzept aus dem Blickwinkel des Arbeitsrechts sowie des Urheberrechts beleuchtet. Am Ende der Darstellung des jeweiligen Rechtsgebietes werden Handlungsempfehlungen beschrieben, die gleichzeitig als eine Art Checkliste genutzt werden können.

I. Arbeitsrecht

Derzeit bestehende Dienst- und Arbeitsverträge sowie Dienst- bzw. Betriebsvereinbarungen beinhalten in der Regel nur die private Nutzung der Kommunikationssysteme des Arbeitgebers mittels dienstlicher Geräte, wohingegen die dienstliche Nutzung dieser Systeme über private Endgeräte (noch) nicht vertraglich geregelt ist. Sofern sich der Arbeitgeber für eine Zulassung von „BYOD“ entscheidet, sind über die bisherigen Regelungen hinausgehende Dienst- bzw. Betriebsvereinbarungen notwendig. Daneben scheint die Anpassung bestehender Dienst- und Arbeitsverträge in Teilen sinnvoll. Im Zuge einer neuen Dienst- bzw. Betriebsvereinbarung können dann auch die datenschutzrechtlichen Belange der Mitarbeiter im Rahmen der §§ 12 Abs. 4, 32 Bundesdatenschutzgesetz (BDSG) (sowie der entsprechenden Vorschriften der Landesdatenschutzgesetze, vgl. § 36 LDSG BW, § 2 Abs. 2 BlnDSG, § 29 BbgDSG, § 20 BrDSG, § 32 HmbDSG, § 34 HDSG, § 35 DSG MV, § 24 NDSG, § 29 DSG NW, § 31 LDSG RP, § 31 SDSG, § 27 SächsDSG, § 28 DSG-LSA, § 23 LDSG SH, § 33 ThürDSG) geregelt werden, welcher die Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses betrifft. Auf die datenschutzrechtlichen Probleme bei der Einführung von „BYOD“ wird allerdings noch in einem gesonderten Beitrag eingegangen.

Bereitstellung betrieblicher Ressourcen

Grundsätzlich trifft den Arbeitgeber die Verpflichtung, betriebliche Ressourcen bereitzustellen und zu erhalten. Die privaten Endgeräte des Arbeitnehmers stehen in seinem Privateigentum. Dieses Privateigentum ist jedoch nicht vom Direktions- bzw. Weisungsrecht des Arbeitgebers umfasst, sodass ein verpflichtender „BYOD"-Einsatz dieser Geräte nicht angeordnet werden kann. Erlaubt der Arbeitgeber die Einbringung eigener Geräte, ist es ratsam, die jeweiligen Gerätetypen und Softwareversionen genau zu bezeichnen und zu dokumentieren. Eines der größten Probleme im Zuge von „BYOD" ist nämlich die Verwaltung unterschiedlichster Mobilgeräte. Es ist daher eine hoch skalierbare Managementplattform erforderlich. Einer unbedingten Regelung bedarf im Zuge der Einführung von „BYOD" aus haftungs- und datenschutzrechtlichen Gründen vor allem die konkrete Abgrenzung zwischen der privaten und betrieblichen Nutzung des eingebrachten Gerätes. Im Rahmen dieser Regelung ist auch eine klare Abgrenzung in zeitlicher Hinsicht angezeigt (zu diesem Punkt sogleich mehr). Auch der Vergütungsanspruch des Arbeitnehmers für die betriebliche Nutzung sollte vertraglich festgelegt werden. Entsprechend des Anteils der Nutzung sind die Kosten dort prozentual aufzuführen, wobei daneben eine Anpassungsklausel ratsam ist. Auf diese Weise kann Veränderungen in der Verteilung dieser Anteile besser nachgekommen werden. Eine anteilige Beteiligung des Arbeitgebers an den Kosten für Anschaffung und Wartung ist denkbar. Der Arbeitgeberanteil kann dabei als pauschale Vergütung oder in Form eines Einzelnachweises abgegolten werden.

Einhaltung der Arbeitszeit

Vor allem aus zeitlicher Sicht muss im Zuge der Einführung von „BYOD" die konkrete Abgrenzung zwischen der privaten und betrieblichen Nutzung des eingebrachten Gerätes geregelt werden. Im Rahmen der heutigen Kommunikation vermengen sich Freizeit und Arbeitszeit in einem zunehmenden Maße. „BYOD"-Programme verstärken diesen Effekt durch die permanente Erreichbarkeit des Arbeitnehmers. Zu nennen ist hier etwa das Lesen dienstlicher E-Mails oder die Annahme von Kunden- sowie Mitarbeiteranrufen in der Freizeit. Dadurch könnte sich der Arbeitnehmer gezwungen fühlen, auch in seiner Freizeit und damit außerhalb der klassischen Arbeitszeit dienstliche Anfragen auf seinem Gerät zu beantworten. Darin kann möglicherweise eine Arbeitsaufnahme zu sehen sein, die arbeitszeitrechtlich relevant ist. Sofern der Arbeitnehmer außerhalb seiner regulären Arbeitszeit zu ständiger Erreichbarkeit auf seinem Endgerät verpflichtet ist, ist dies arbeitsrechtlich als Rufbereitschaft einzuordnen. Er muss nämlich zur Arbeitsaufnahme an einem Ort seiner Wahl außerhalb der Arbeitszeit auf Abruf stehen. Zu beachten ist aber, dass die Arbeitszeit erst ab der tatsächlichen Arbeitsaufnahme beginnt. Die Rufbereitschaft als solche ist dagegen noch nicht als Arbeitszeit einzuordnen. Eine Rufbereitschaft wird aber dann nicht vorliegen, wenn der Arbeitnehmer nicht zur ständigen Erreichbarkeit verpflichtet ist. Sofern der Mitarbeiter freiwillig außerhalb seiner regulären Arbeitszeit tätig wird, kann darin grundsätzlich keine Arbeitszeit gesehen werden. Dementsprechend sind klare und verlässliche Regelungen zum arbeitszeitlichen Umgang mit den privaten Geräten außerhalb der vereinbarten Arbeitszeit sowie zum privaten Gebrauch während der Arbeitszeit festzulegen. Dies gilt insbesondere vor dem Hintergrund des § 5 Arbeitszeitgesetz (ArbZG), wonach die Arbeitnehmer nach Beendigung der täglichen Arbeitszeit eine ununterbrochene Ruhezeit von mindestens elf Stunden haben müssen. Ferner ist zu beachten, inwieweit der Arbeitnehmer Überstunden ableisten muss und wie diese vergütet oder durch Freizeitausgleich abgegolten werden.

Beteiligung des Personalrats bzw. des Betriebsrats

Aus arbeitsrechtlicher Perspektive ist im öffentlichen Sektor auch die Beteiligung des Personalrats von entscheidender Bedeutung. Eine Mitbestimmungspflicht des Personalrats kann sich bei der Einführung dementsprechend aus folgenden Vorschriften (sowie den entsprechenden Vorschriften der Landespersonalvertretungsgesetze) ergeben:

- § 75 Abs. 3 Nr. 15 Bundespersonalvertretungsgesetz (BPersVG) (Regelung der Ordnung in der Dienststelle und des Verhaltens der Beschäftigten);
- § 75 Abs. 3 Nr. 16 BPersVG (Gestaltung der Arbeitsplätze);
- § 75 Abs. 3 Nr. 17 BPersVG (Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen);
- § 76 Abs. 2 Nr. 7 BPersVG (Einführung grundlegend neuer Arbeitsmethoden).

Im nicht-öffentlichen Bereich müssen die Vorschriften des Betriebsverfassungsgesetzes (BetrVG) beachtet werden. Zunächst hat der Betriebsrat ein Kontrollrecht nach § 80 BetrVG,

wozu nach § 80 Abs. 1 Nr. 1 BetrVG etwa die Überwachung der Einhaltung der zugunsten der Arbeitnehmer geltenden Gesetze durch den Arbeitgeber zählt. Daneben kann sich eine Mitbestimmungspflicht des Betriebsrates insbesondere aus folgenden Gründen ergeben:

- § 87 Abs. 1 Nr. 1 BetrVG: Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb, etwa im Hinblick auf Passwortverwaltung, Malwareschutz oder Updates;
- § 87 Abs. 1 Nr. 2 BetrVG: Beginn und Ende der täglichen Arbeitszeit einschließlich der Pausen sowie Verteilung der Arbeitszeit auf die einzelnen Wochentage, insbesondere mit Blick auf die Always-on-Connectivity, wodurch eine Vermischung von Arbeits- und Freizeitgestaltung erfolgt;
- § 87 Abs. 1 Nr. 3 BetrVG vorübergehende Verkürzung oder Verlängerung der betriebsüblichen Arbeitszeit;
- § 87 Abs. 1 Nr. 6 BetrVG: Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Hierbei ist die Geeignetheit zur Überwachung ausreichend, sodass der Arbeitgeber nicht gezielt Überwachungszwecke verfolgen muss. Eine solche Eignung zur Überwachung kann zum Beispiel schon vorliegen beim Protokollieren von Logins, Synchronisationsvorgängen, GPS-Lokalisierungsdaten sowie bei datenschutzrechtlichen Kontrollbefugnissen.

Gegenstand dieses Mitbestimmungsrechts können beispielsweise der Zeitpunkt der Einführung von „BYOD“, der Zeitraum der Nutzung und die überbetriebliche Vernetzung sein. Nach § 90 BetrVG bestehen im Hinblick auf die Planung von technischen Anlagen (§ 90 Abs. 1 Nr. 2 BetrVG), von Arbeitsverfahren und Arbeitsabläufen (§ 90 Abs. 1 Nr. 3 BetrVG) und der Arbeitsplätze (§ 90 Abs. 1 Nr. 4 BetrVG) Unterrichtungspflichten gegenüber dem Betriebsrat. Daher muss der Arbeitgeber den Betriebsrat bereits im Planungsstadium hinsichtlich der Gestattung von „BYOD“ einbeziehen und diesen unter Vorlage der erforderlichen Unterlagen unterrichten.

Handlungsempfehlungen

Wie deutlich gemacht wurde, gilt es auch aus arbeitsrechtlicher Sicht einige Punkte zu beobachten, um eine rechtmäßige Einführung von „BYOD“ zu gewährleisten. Die nachfolgende Darstellung der Handlungsempfehlungen soll gleichzeitig als eine Art Checkliste dienen.

1. Als oberstes Gebot gilt vorweg, dass aus Gründen der Rechtssicherheit, Klarheit und Transparenz sämtliche Absprachen zwischen Arbeitgeber und Arbeitnehmer schriftlich festgehalten werden sollten. Bisher bestehende Dienst- bzw. Betriebsvereinbarungen sowie Dienst- und Arbeitsverträge werden keine Passus zum Themenkomplex „BYOD“ beinhalten. Daher sollten diese um entsprechende Abschnitte ergänzt werden, wobei in diesem Zusammenhang direkt auch datenschutzrechtliche Belange der Mitarbeiter konstituiert werden können. Neben Dienst- bzw. Betriebsvereinbarungen sollte daher auf Individualvereinbarungen zurückgegriffen werden. Es gilt zu beachten, dass Dienst- bzw. Betriebsvereinbarungen BDSG- und AGB-fest sein müssen (vgl. insbesondere §§ 305c Abs. 2, 307 Abs. 1 S. 2 Bürgerliches Gesetzbuch (BGB)). Dennoch sind Dienst- bzw. Betriebsvereinbarungen das „Mittel der Wahl“ bei fast allen Fragen mobiler Endgeräte in der jeweiligen Einrichtung, da mit ihnen einige Vorteile einhergehen. Es können verbindliche Vereinbarungen über sämtliche Gegenstände betrieblicher Mitbestimmung getroffen werden (vgl. § 77 Abs. 4 S. 1 BetrVG, wonach Betriebsvereinbarungen unmittelbar und zwingend gelten). Das BPersVG sowie weitestgehend die Personalvertretungsgesetze der Länder kennen keine solche Vorschrift, die Dienstvereinbarungen für unmittelbar und zwingend erklärt (vgl. § 73 BPersVG). Der Gesetzgeber hat es anscheinend als selbstverständlich angesehen, dass auch Dienstvereinbarungen unmittelbar und zwingend gelten. Dementsprechend kann § 77 Abs. 4 S. 1 BetrVG entsprechend angewendet werden. Gleichzeitig können mögliche Probleme der AGB-Inhaltskontrolle abgemildert werden (§ 310 Abs. 4 BGB). Da eine wirksame Betriebsvereinbarung zugleich als Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG gilt (vgl. die entsprechenden Vorschriften der Landesdatenschutzgesetze: § 4 Abs. 1 LDSG BW, Art. 15 Abs. 1 BayDSG, § 6 Abs. 1 BlnDSG, § 4 Abs. 1 BbgDSG, § 3 Abs. 1 BrDSG, § 5 Abs. 1 S. 1 HmbDSG, § 7 Abs. 1 HDSG, § 7 Abs. 1 DSG MV, § 4 Abs. 1 NDSG, § 4 Abs. 1 DSG NW, § 5 Abs. 1 LDSG RP, § 4 Abs. 1 S. 1 SDSG, § 4 Abs. 1 SächsDSG, § 4 Abs. 1 DSG-LSA, § 11 Abs. 1 LDSG SH, § 4 Abs. 1 ThürDSG), können datenschutzrechtliche Befugnisse des Arbeitgebers darin verankert werden, ohne auf eine Einwilligung des Arbeitnehmers angewiesen zu sein. Es muss aber beachtet werden, dass nur Pflichten des Arbeitgebers sowie Pflichten des Arbeitnehmers im Hinblick auf die Verbindung zur IT-Infrastruktur der jeweiligen Einrichtung festgelegt werden können, wohingegen Aspekte

des Privatlebens des Arbeitnehmers (etwa Vorschriften über den Abschluss von Reparatur-, Wartungs- und Garantieverträgen, Software- und Hardwareanschaffung) darin nicht geregelt werden können und dafür daher individualvertragliche Vereinbarungen erforderlich sind.

2. Zur Verwaltung der im Rahmen von „BYOD“ in einer Vielzahl eingebrachten Endgeräte der Arbeitnehmer sollten die jeweiligen Gerätetypen und Softwareversionen genau bezeichnet und dokumentiert werden. Hierbei bietet sich eine hoch skalierbare Managementplattform an. Individualvertragliche Regelungen sollten in diesem Zusammenhang neben sämtlichen Kostenfragen im Hinblick auf Anschaffung, Wartung, Reparatur und Ersatz auch den Vergütungsanspruch des Arbeitnehmers für die betriebliche Nutzung beinhalten. Die Kosten sind dabei entsprechend des Anteils der jeweiligen Nutzung (dienstlich und privat) prozentual aufzuführen, wobei daneben eine Anpassungsklausel ratsam ist, da auf diese Weise Veränderungen in der Verteilung dieser Anteile besser nachgekommen werden kann.

3. Die Vorgaben hinsichtlich der Arbeitszeit müssen unbedingt beachtet und dementsprechende Regelungen zwischen den Parteien getroffen werden, damit keine Vermengung von Arbeitszeit und Freizeit erfolgt. Bei der Einführung von „BYOD“ sollte aus arbeitszeitrechtlicher Sicht insbesondere auf eine Verpflichtung der Arbeitnehmer zu einer ständigen Erreichbarkeit außerhalb der regulären Arbeitszeiten verzichtet werden. Dementsprechend sind klare und verlässliche Regelungen sowohl zum arbeitszeitlichen Umgang mit den privaten Geräten außerhalb der vereinbarten Arbeitszeit als auch hinsichtlich des privaten Gebrauchs während der Dienstzeit festzulegen. Hierbei können die üblichen arbeitsrechtlichen Maßstäbe zur Online-Nutzung am Arbeitsplatz als Richtwerte dienen, wobei es zu beachten gilt, dass ein zu strenges Management seitens des Arbeitgebers die Begeisterung der Arbeitnehmer für „BYOD“ schwinden lassen kann. Empfehlenswert sind Regelungen, durch die der Arbeitnehmer zur Einhaltung der Ruhezeiten nach § 5 ArbZG angehalten wird, wobei meist auch seitens des Personal- bzw. Betriebsrats dahingehende Forderungen aufkommen. Sofern absehbar ist, dass ein phasenweises Tätigwerden des Arbeitnehmers außerhalb seiner regulären Arbeitszeit unausweichlich ist und dies sogar vom Arbeitgeber veranlasst wird (etwa die Weiterleitung einer E-Mail mit der Aufforderung zur Beantwortung, das Durchleiten eines Anrufs oder die Ansetzung einer Telefon-/Videokonferenz), sollte dies ausdrücklich geregelt werden. Neben dem Arbeitszeitgesetz kommen im Rahmen von „BYOD“ auch Fragen hinsichtlich der Ableistung und Vergütung bzw. Abgeltung von Überstunden auf. Diese Punkte können im Verlauf eines „BYOD“-Programms zu Streitigkeiten führen, sodass hier idealerweise schon im Vorfeld unter Beteiligung der betroffenen Kreise (Arbeitgeber sowie Arbeitnehmervertreter) interessengerechte und eindeutige Regelungen geschaffen werden sollten.

4. Die Einführung von „BYOD“ wird regelmäßig die Mitwirkung des Personalrats (im öffentlichen Bereich) sowie des Betriebsrats (im nicht-öffentlichen Bereich) zur Folge haben. Aufgrund bestehender Unterrichtungspflichten und zur Vermeidung von Verlangsamungs- oder Verhinderungsmaßnahmen ist eine frühzeitige Einbindung dieser Organe (schon im Planungsstadium) ratsam (vgl. die oben genannten Vorschriften). Durch eine offene und transparente Vorgehensweise seitens des Arbeitsgebers können Vorbehalte und Befürchtungen frühzeitig aufgeklärt und beiseite geschafft werden.

II. Urheberrecht

Auf den ersten Blick mag es befremdlich erscheinen, was das Urheberrecht mit dem Thema „BYOD“ zu tun haben kann. Schließlich bringen die Mitarbeiter ihre bereits funktionsfähigen Endgeräte am Arbeitsplatz ein. Es bestehen jedoch einige Fallstricke aus urheberrechtlicher Sicht, die es zu beachten gilt. Bei der Einbringung seiner Geräte samt Software geht das Eigentum daran nicht auf den Arbeitgeber über. Vielmehr bleibt der Arbeitnehmer weiterhin deren Eigentümer. Dies gilt auch im Falle der betrieblichen Nutzung dieser Endgeräte. Von dieser Eigentumslage sind aber die Nutzungsrechte an der installierten Software zu unterscheiden und müssen gesondert betrachtet werden.

Unterlizenzierung

Sobald der Arbeitnehmer private Endgeräte mit installierter Software für dienstliche Zwecke nutzt, können der Arbeitgeber und der Arbeitnehmer in Konflikt mit dem Urheberrecht kommen. Bei jedem Einsatz von Software müssen die ent-

sprechenden Nutzungsrechte eingehalten werden. Meistens beziehen sich die Nutzungsrechte nur auf eine bestimmte Nutzungsart. Die auf dem privaten Endgerät installierte Software ist häufig lediglich auf die private Nutzung ausgerichtet und daher vom Hersteller ausschließlich zu diesem Zweck lizenziert. Die Lizenzbedingungen erlauben in diesem Fall regelmäßig eine dienstliche Nutzung der Software nicht. Anbieter von Freeware und Cloud-Anwendungen sehen in ihren Lizenzbedingungen üblicherweise besondere Modelle für die dienstliche Nutzung ihrer Produkte vor. Entsprechendes kann auch im umgekehrten Fall gelten, wenn also die durch den Unternehmer lizenzierte Software auf den privaten Geräten installiert wird und dann vom Arbeitnehmer auch privat genutzt wird. Die Konsequenz beider Konstellationen ist eine Unterlizenzierung hinsichtlich der installierten Software.

Der Arbeitnehmer wird die für die dienstliche Nutzung lizenzierte Software häufig auch privat nutzen und umgekehrt für private Zwecke erworbene Software gleichzeitig für dienstliche Angelegenheiten einsetzen. Dabei kann es teilweise vorkommen, dass die ursprünglich im Privatbereich genutzte Software, die im Zuge von „BYOD“ für dienstliche Zwecke verwendet wird, gar nicht lizenziert ist. Dadurch kann es zu verbotenen und strafbaren Verhaltensweisen in Form von vergütungsrelevanten Nutzungshandlungen sowie urheberrechtlich relevanten Vervielfältigungen und Weitergaben kommen. In diesem Zusammenhang kann gerade die dienstliche Nutzung der Software als solche bereits die Verletzungshandlung darstellen. Dementsprechend muss auf die konkrete Ausgestaltung der Lizenzbestimmungen geachtet werden, insbesondere auf die Unterscheidung zwischen privaten und gewerblichen Nutzungsbefugnissen, aber auch zwischen personen- oder gerätegebundenen Lizenzen sowie Mehrplatzlizenzen. Zur Kontrolle und zum Ausschluss einer Unterlizenzierung seitens des Arbeitgebers sind daher regelmäßige interne Audits unabdingbar.

Die soeben beschriebenen Handlungen können je nach Konstellation (insbesondere Umfang und Dauer der Unterlizenzierung) für Arbeitgeber und Arbeitnehmer erhebliche zivilrechtliche Folgen haben. So besteht zunächst ein Anspruch auf Schadensersatz und Unterlassung sowie Beseitigung gegen die handelnde Person aus § 97 UrhG. Nach § 99 UrhG haftet der Unternehmer verschuldensunabhängig für die Urheberrechtsverletzungen seiner Mitarbeiter. „Unternehmer“ i. S. d. § 99 UrhG sind dabei auch Körperschaften des öffentlichen Rechts, also z.B. Hochschulen. Die Formulierung „in einem Unternehmen“ in § 99 UrhG ist zur Gewährleistung eines wirksamen Rechtsschutzes funktional sowie weit zu verstehen und bedeutet, dass die Verletzungshandlung des Mitarbeiters im Tätigkeitsbereich der jeweiligen Einrichtung erfolgen muss. Diese Voraussetzung ist bereits dann erfüllt, wenn der Arbeitgeber „BYOD“ gestattet. Zu beachten sind zudem die Straf- und Bußgeldvorschriften der §§ 106 ff. UrhG, die für rechtswidrige Vervielfältigungshandlungen eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe vorsehen. Daneben kann mit einem Bekanntwerden von massiven Lizenzverstößen durch eine Einrichtung unabhängig davon, ob diese bewusst oder unbewusst erfolgten, ein hoher Ansehensverlust einhergehen.

Software aus zweifelhaften Quellen

Aus dem Blickwinkel der IT-Sicherheit weitaus gefährlicher als die soeben dargestellte Unterlizenzierung ist die Verwendung von illegaler Software aus zweifelhaften Quellen. Der Download von Software durch den Arbeitnehmer kann grundsätzlich nicht eingeschränkt werden. Daher kann es (insbesondere aus Kostengründen) möglich sein, dass der Arbeitnehmer nicht-lizenzierte Softwareversionen von Internetseiten herunterlädt, die vom Hersteller nicht mit der Verbreitung der Software betraut wurden. Meist handelt es sich dabei um genuin urheberrechtswidrig erstellte Kopien ohne jede Art von Lizenz, sodass das soeben besprochene Problem der Unterlizenzierung hier fortbesteht. Der Arbeitgeber hat kaum Kontrollmöglichkeiten über die herangezogenen Quellen, insbesondere wenn der Arbeitnehmer den Download und die Installation zu Hause durchführt. In vielen Fällen sind die aus diesen zweifelhaften Quellen bezogenen Softwareprodukte virenbehaftet oder „gehackt“. Aufgrund der erhöhten Anfälligkeit für Hacker- oder Virenangriffe bedeutet die Verwendung dieser Software eine erhöhte Gefahr für die IT- und Unternehmenssicherheit.

Handlungsempfehlungen

Bei Urheberrechtsverletzungen können neben Unterlassungs- und Beseitigungsansprüchen (§ 97 Abs. 1 UrhG) auch Schadensersatzansprüche (§ 97 Abs. 2 UrhG) auf den Verletzer zukommen, die gerade im Softwarebereich mit erheblichen Summen verbunden sein können und die Gefahr von Abmahnungen bergen. Daneben dürfen auch die speziellen Straf- und Bußgeldvorschriften (§§ 106 ff. UrhG) nicht aus dem Blickfeld verschwinden, die im Verletzungsfall empfindliche Strafen

vorsehen. Dementsprechend sind zur Vorbeugung von Haftungsfällen aus dem urheberrechtlichen Bereich im Vorfeld einige Maßnahmen zu ergreifen, damit die Gefahren möglichst gering gehalten werden und die Einführung von „BYOD“ somit erleichtert wird. Die nachfolgende Darstellung der Handlungsempfehlungen dient wiederum als eine Art Checkliste.

1. Zur Verhinderung von urheberrechtlichen Verletzungshandlungen durch Unterlizenzierung muss auf die konkrete Ausgestaltung der Lizenzbestimmungen geachtet werden, insbesondere auf die Unterscheidung zwischen privaten und gewerblichen Nutzungsbefugnissen, aber auch zwischen personen- oder gerätegebundenen Lizenzen sowie Mehrplatzlizenzen. Diesbezüglich müssen seitens des Arbeitgebers regelmäßige interne Audits durchgeführt werden. Auf diese Weise kann einerseits kontrolliert werden, welche Softwares auf den privaten Endgeräten installiert sind, andererseits kann dadurch eine Unterlizenzierung verhindert werden. Die internen IT-Richtlinien sollten auf die Lizenzneuerungen im Zuge von „BYOD“ angepasst und deren Einhaltung regelmäßig überprüft werden.

2. Daneben sollte zur Minimierung des Haftungsrisikos für Urheberrechtsverletzungen sowie der aus Schadsoftware herrührenden Gefahren das betriebliche Lizenzmanagement auf die privaten Geräte in betrieblicher Nutzung erstreckt werden. Idealerweise sollten die Endgeräte der Mitarbeiter regelmäßig auf unlizenzierte, illegale oder schädliche Software überprüft werden. Dies könnte in einer Betriebsvereinbarung geregelt werden (siehe dazu bereits die obigen Ausführungen). Es erscheint jedoch unwahrscheinlich, dass ein Mitarbeiter den gesamten Inhalt seines Gerätes ohne weiteres offenlegen wird. Der Schutz der Privatsphäre der Arbeitnehmer sollte vom Arbeitgeber gefördert werden, da so mögliche Vorbehalte gegen eine Einführung von „BYOD“ abgemildert werden. Daher könnte man alternativ zu einer vollumfänglichen Offenlegungspflicht den Mitarbeiter dazu verpflichten, in regelmäßigen Abständen einen Nachweis über die ordnungsgemäße Lizenzierung der von ihm zu betrieblichen Zwecken eingesetzten Software zu erbringen. Mit dem Einverständnis des Mitarbeiters könnte man diesen Nachweis durch eine stichprobenartige Überprüfung absichern. Sofern der Arbeitnehmer derartige Überprüfungen verweigert, sollte das private Gerät nicht betrieblich verwendet werden dürfen, was einem Widerruf von „BYOD“ in Bezug auf diesen Arbeitnehmer bedeutet. Eine sehr strikte Regelung könnte daneben vorschreiben, welche Software der Mitarbeiter auf dem dienstlichen Bereich seines Endgeräts (dazu sogleich mehr) installieren darf und dass dahingehende Kontrollen erlaubt sind. Bestehende Gewährleistungsansprüche für die eingesetzten Softwares könnten an den Arbeitgeber abgetreten oder für den Arbeitgeber geltend gemacht werden. Alternativ bieten sich auch der zentrale Einkauf sowie die Verwaltung der erforderlichen Softwares durch den Arbeitgeber an. Er kann diese direkt in sein betriebliches Lizenzmanagement einpflegen und verringert auf diese Weise die Gefahr einer Unterlizenzierung deutlich. Dabei sollte auch darauf geachtet werden, dass die erworbenen Nutzungsrechte sowohl die dienstliche als auch die private Nutzung der jeweiligen Software erlauben. Dadurch möglicherweise entstehende Mehrkosten können interessengerecht zwischen Arbeitgeber und Arbeitnehmer aufgeteilt werden, sofern die private Nutzung möglich ist, einen merklichen Anteil trägt und sich der Arbeitnehmer bewusst und freiwillig zur Teilnahme am BYOD-Programm entscheidet. Um Konflikte zu vermeiden, sollte die Kostenaufteilung schriftlich fixiert werden. Letztlich kann auch die Nutzung von Open-Source-lizenzierter Software eine Option sein.

3. Die Trennung von privaten und dienstlichen Daten auf technischer Ebene erscheint unabdingbar, um die notwendigen Kontrollmöglichkeiten seitens des Arbeitgebers umzusetzen. In diesem Zusammenhang ist an die Konfiguration virtueller Desktops (= multiple Arbeitsflächen (-bereiche)), die Partitionierung der Festplatten der Geräte, verschlüsselte Container (Container-Apps) oder Terminalserver-Lösungen zu denken. Auf diese Weise kann einerseits eine Kontrolle erfolgen, ohne dass private Daten des Arbeitnehmers betroffen wären, andererseits könnte illegal installierter Software der Zugriff auf das Unternehmensnetzwerk verweigert werden.

Anmerkung:

Einen ausführlichen Leitfaden zur Handhabung von „Bring Your Own Device“ finden Sie unter: https://www.dfn.de/fileadmin/3Beratung/Recht/handlungsempfehlungen/BYOD-Leitfaden.pdf

Ein Auskunftsverlangen, das man nicht ablehnen kann

Zum Auskunftsanspruch gegen Host-Provider bei Urheberrechtsverletzungen durch Dritte

von Lennart Sydow

Das Landgericht Hamburg hatte in einem Verfahren im einstweiligen Rechtsschutz vom 12.01.2015 (Az.: 310 O 11/15) über die Verpflichtung eines Webhosting-Anbieters zur Erteilung von Auskünften über seine Nutzer zu entscheiden. Solche Auskunftsansprüche gegen Dritte, die selbst nicht für die eigentliche Urheberrechtsverletzung verantwortlich sind, bestehen nur in wenigen gesetzlich geregelten Fällen. Die gewerbliche Erbringung von Dienstleistungen, die für rechtsverletzende Tätigkeiten genutzt werden, ist einer davon. Hochschulen und Forschungseinrichtungen müssen sich daher mit dem möglichen Eingang etwaiger Auskunftsersuchen beschäftigen, wenn sie als Internetzugangsanbieter auftreten oder Dritten Speicherkapazitäten zur Verfügung stellen.

I. Hintergrund

Die rechtswidrige Verbreitung von Software und Medieninhalten, wie Foto-, Film- und Musikdateien, über das Internet, ist vor deutschen Gerichten seit Jahren ein ständig aktuelles Thema. Aus rechtlicher Sicht steht dem Urheber allein das Recht zu, sein Werk über das Internet öffentlich zugänglich zu machen. Diese Inhalte können nur zulässigerweise im Internet zugänglich gemacht werden, wenn entweder eine der gesetzlichen Schrankenregelungen dies erlaubt oder der Urheber Nutzungsrechte daran eingeräumt hat. Anderenfalls stellt die Zugänglichmachung durch Dritte eine Urheberrechtsverletzung dar. Für die Rechteinhaber ist es aber oft mit erheblichen Schwierigkeiten verbunden, gegen die Verantwortlichen vorzugehen. Zwar besteht gegen die Täter und Teilnehmer einer Urheberrechtsverletzung ein Anspruch auf Unterlassung der verletzenden Handlung und im Falle einer vorsätzlichen oder fahrlässigen Verletzung auch ein Anspruch auf Schadensersatz aus § 97 Urheberrechtsgesetz (UrhG). Um diese Rechte aber durchzusetzen, ist zunächst einmal erforderlich, dass dem Rechteinhaber die Identität der handelnden Personen bekannt ist. Dies ist bei Rechtsverletzungen im Internet für die Rechteinhaber nur schwer festzustellen. Damit sie an die nötigen Informationen gelangen können, hat der Gesetzgeber in § 101 Abs. 2 UrhG unter gewissen Voraussetzungen einen Auskunftsanspruch gegen Personen vorgesehen, die nicht selbst eine Urheberrechtsverletzung vornehmen oder daran teilnehmen, sondern nur eine (technische) Hilfstätigkeit ausüben.

Nach dieser Vorschrift kann die Herausgabe verschiedener Informationen, wie beispielsweise der Name und die Anschrift der Nutzer einer Dienstleistung, verlangt werden. Der Auskunftsanspruch richtet sich unter anderem gegen denjenigen, der in gewerblichem Ausmaß Dienstleistungen erbracht hat, die für rechtsverletzende Tätigkeiten genutzt wurden. Erforderlich ist darüber hinaus, dass eine offensichtliche Urheberrechtsverletzung vorliegt und dass das Auskunftsverlangen im Einzelfall nicht unverhältnismäßig ist. Soweit Verkehrsdaten – also solche Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (siehe § 3 Nr. 30 Telekommunikationsgesetz) – verwendet werden müssen, um die Auskunft erteilen zu können, ist zudem eine richterliche Anordnung über die Zulässigkeit der Auskunftserteilung erforderlich.

Immer wieder haben sich Gerichte diesbezüglich damit zu beschäftigen, dass Accessprovider, als gewerbliche Anbieter von Dienstleistungen, zur Erteilung von Auskünften über ihre Nut-

zer verpflichtet werden sollen (siehe hierzu: Klein, „Verfolgung von Urheberrechtsverletzungen im Internet erleichtert“, DFN-Infobrief Recht 5/2012).

Anfang dieses Jahres hatte das Landgericht Hamburg (LG Hamburg) nun in einem Verfahren über einen solchen Auskunftsanspruch gegen einen Webhosting-Anbieter zu entscheiden, der dem Betreiber eines BitTorrent-Trackers nicht den Netzzugang aber Serverkapazitäten zur Verfügung stellte. BitTorrent ist eines der größten Filesharing-Netzwerke, bei dem eine Inhaltsdatei in Datenpakete aufgeteilt und dann direkt zwischen Nutzern weiterverteilt wird.

II. Sachverhalt und Entscheidung des Gerichts

In dem Beschluss des LG Hamburg vom 12.01.2015 (Az.: 310 O 11/15) ging es um einen Fall, in dem die Anwälte der Rechteinhaber zunächst die Betreiber dreier großer BitTorrent-Tracker aufgefordert hatten, Inhalte ihrer Mandanten zu sperren. Tracker sind spezielle Server, die den Kontakt zwischen Teilnehmern des BitTorrent-Netzwerkes herstellen und diesen so ermöglichen, einzelne Datenpakete auszutauschen, die dann wieder zu der Inhaltsdatei zusammengesetzt werden. Sie vermitteln die Kontaktaufnahme zwischen den Nutzern des Netzwerkes, indem sie die IP-Adressen der anbietenden Rechner an den suchenden Rechner senden. Als diese nicht auf die Aufforderung reagierten, wendeten die Rechteinhaber sich an den Webhosting-Anbieter der Tracker-Server und wiesen ihn auf die rechtsverletzenden Inhalte hin. Als Hostprovider ist ein solcher Webhosting-Anbieter grundsätzlich nicht Täter oder Teilnehmer einer Rechtsverletzung, die von seinen Kunden unter Nutzung der von ihm zur Verfügung gestellten Speicherkapazitäten begangen wird. Möglich ist aber eine Verpflichtung zur Unterlassung nach den Grundsätzen der Störerhaftung, wenn der Anbieter in irgendeiner Weise willentlich und adäquat kausal zur Verletzung eines geschützten Rechtsgutes beiträgt und zumutbare Prüfpflichten verletzt hat. Um eine solche Verantwortlichkeit als Störer zu vermeiden, schaltete der Provider die Server der betroffenen Seiten auf den Hinweis der Rechteinhaber ab, nachdem er zunächst die Betreiber der Tracker-Server aufgefordert hatte, die rechtsverletzenden Inhalte zu sperren, diese aber darauf nicht reagiert hatten.

Da der Webhosting-Anbieter seinen Pflichten unverzüglich nachkam, war eine gerichtliche Geltendmachung eines Unterlassungsanspruchs gegen diesen nicht erforderlich. Sein Beitrag an der Rechtsverletzung des Tacker-Servers wurde beseitigt. Vor das LG Hamburg gelangte der Fall erst, weil die Rechteinhaber noch zusätzlich Auskunft über Namen, Anschrift und E-Mail-Adresse der Kunden des Providers verlangten, die die Tracker-Server bis zu diesem Zeitpunkt betrieben hatten. Der Anspruch zur Erteilung von Auskünften ist unabhängig von der Verpflichtung zur Unterlassung der störenden Handlung, die zu der Rechtsverletzung beiträgt. Da der Anbieter diese Auskünfte verweigerte, beantragten die Rechteinhaber vor dem LG Hamburg, dem Hostprovider die Erteilung der Auskünfte aufzugeben. Das Gericht folgte dem Antrag und stellte die Verpflichtung des Webhosting-Anbieters zur Auskunftserteilung fest, weil alle Voraussetzungen des § 101 Abs. 2 UrhG erfüllt seien: Die Rechteinhaber hatten aus Sicht der Richter glaubhaft gemacht, dass MP3-Dateien von Musikstücken, an denen sie die ausschließlichen Nutzungsrechte halten, im Internet unerlaubterweise öffentlich zugänglich gemacht worden waren. Dies sei unter Verwendung der fraglichen Tracker-Server geschehen, die die Verbindung zu den Nutzern herstellten. Sobald die Verbindung hergestellt worden war, wurden die Inhalte von verschiedenen Nutzern heruntergeladen. Der Zugriff sei somit unter Verwendung der Tracker-Server ermöglicht worden, auch wenn die Inhalte selbst nicht auf diesen hinterlegt waren. Dies wertete das Gericht als ausreichend für die erforderliche offensichtliche Rechtsverletzung. Auch habe der Webhosting-Dienst mit der Zurverfügungstellung der Serverkapazitäten in gewerblichem Ausmaß eine Dienstleistung erbracht, welche für die rechtsverletzenden Tätigkeit der Tracker-Server-Betreiber genutzt wurde.

III. Fazit und Auswirkungen für Hochschulen und Forschungseinrichtungen

Diese Einordnung zeigt, dass nicht nur die Internetzugangsanbieter von Nutzern, die Inhalte im Internet verfügbar machen, in Form einer Auskunftsverpflichtung zur Verantwortung gezogen werden können, sondern auch Serverbetreiber, die den rechtsverletzenden Inhalten ähnlich nahe stehen. Leider nicht ganz eindeutig sind die Ausführungen bezüglich der offensichtlichen Rechtsverletzung, die Voraussetzung für den Auskunftsanspruch ist. Hier ist wohl davon auszugehen, dass den Betreibern der Tracker-Server nicht selbst eine Täterschaft oder Teilnahme an den jeweiligen Rechtsverletzungen vorgeworfen wird, denn die Inhaltsdateien werden ausschließlich von den jeweiligen Nutzern geteilt. Die Tracker-Server stel-

len lediglich die Verbindung zwischen Nutzern her, die dann untereinander die Datenpakete austauschen. Von daher ist anzunehmen, dass hier eine Verantwortlichkeit der Tracker ebenfalls nur nach den Grundsätzen der Störerhaftung bestehen kann, wenn diese willentlich einen kausalen Beitrag zur Verletzung leisten. Wann genau der Betreiber eines solchen Tracker-Servers aber verantwortlich ist, kann an dieser Stelle offen bleiben. Für Hochschulen und Forschungseinrichtungen spielt dies praktisch wohl kaum eine Rolle, da sie keine solchen Server betreiben.

Viel relevanter kann für Hochschulen und Forschungseinrichtungen die oben geschilderte Verpflichtung eines Webhosting-Anbieters zur Auskunftserteilung über seine Nutzer sein, auf die diese Entscheidung aufmerksam macht. Dass diese Einrichtungen Speicherkapazitäten für Dritte anbieten, ist in verschiedenen Situationen denkbar und in der Hochschulpraxis stellenweise bereits umgesetzt (zum Beispiel bei Cloud-Diensten für Studenten), wenn auch noch nicht so verbreitet wie das Angebot eines Internetzugangs. Es ist folglich damit zu rechnen, dass im Einzelfall auch gegen Hochschulen in ihrer Funktion als Access- und Hostprovider diese Auskunftsansprüche geltend gemacht werden können. Soweit im Einzelfall solche Auskunftsersuchen gestellt werden, ist zu beachten, dass diese möglichst erst nach einer Prüfung der Voraussetzungen erfüllt werden sollten. Dies gilt zumindest dann, wenn – wie im vorliegenden Fall – keine Verkehrsdaten verwendet werden müssen, um die Auskunft zu erteilen, und daher auch keine richterliche Anordnung erforderlich ist. Besonderes Augenmerk dürfte dabei auf die Frage zu legen sein, ob die Speicherung bestimmter Inhalte durch die Nutzer tatsächlich eine offensichtliche Rechtsverletzung darstellt. Es ist dann jedenfalls zu empfehlen, den Datenschutzbeauftragten und die jeweilige Rechtsabteilung einzubinden.

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