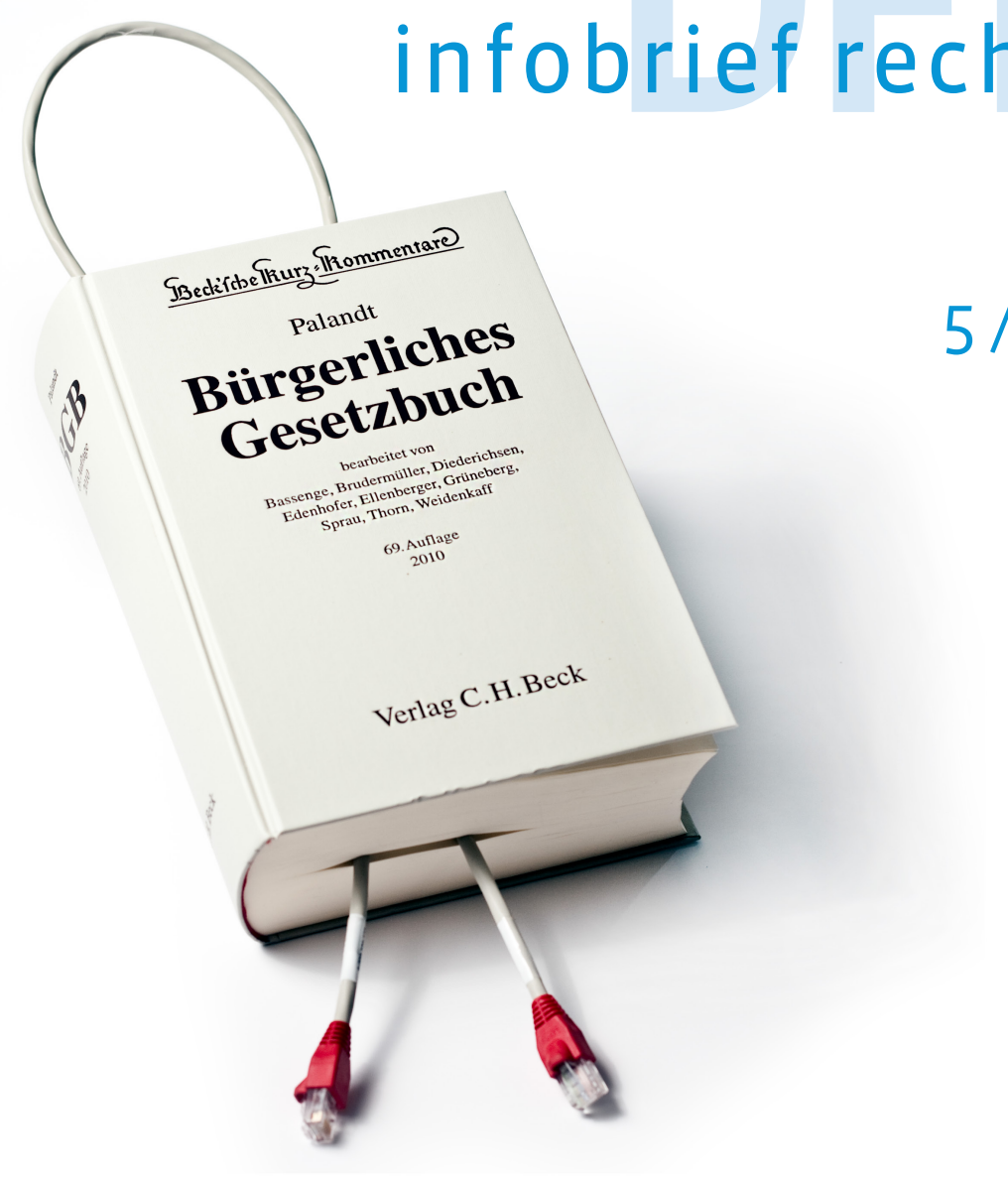
infobrief recht

5 / 2018
Mai 2018



Immer raus mit der Sprache
Auskunftsansprüche gegen Internet-Provider aus dem Urheberrecht

Weiterleiten zur Kündigung
Rechtsprechung zum Arbeitsrecht in Kürze: E-Mail-Weiterleitung als außerordentlicher Kündigungsgrund

Wer hat an der Uhr gedreht?
Statusmeldung zum gegenwärtigen Stand der Umsetzungsgesetze der Länder zur DSGVO

Immer raus mit der Sprache

Auskunftsansprüche gegen Internet-Provider aus dem Urheberrecht

von Marten Tiessen

Durch die kurze Speicherdauer von Verkehrsdaten ist die Verfolgung von Urheberrechtsverletzungen im Internet schwierig. Auch ein Auskunftsanspruch gegenüber dem Internet-Provider ist wirkungslos, wenn dieser die Verkehrsdaten bereits gelöscht hat. In einem Urteil vom 21.09.2017 entschied der Bundesgerichtshof (BGH), dass in Fällen offensichtlicher Rechtsverletzungen bis zum Abschluss eines Gestattungsverfahrens nach § 101 Abs. 9 UrhG der Internet-Provider verpflichtet ist, die Löschung der von ihm erhobenen Verkehrsdaten zu unterlassen, um einen möglichen Auskunftsanspruch zu gewährleisten. Diese Aufbewahrungspflicht kann auch Hochschulen, die als Internet-Provider Dienste anbieten, treffen.

I. Hintergrund

Mit § 101 UrhG besteht im Urheberrecht ein Auskunftsanspruch, der den Urhebern und anderen Rechteinhabern bei der Durchsetzung von Schadensersatz-, Beseitigungs- oder Bereicherungsansprüchen helfen soll. Der Verletzte erhält dabei unter anderem Auskunft über die Herkunft und den Vertriebsweg von rechtsverletzenden Vervielfältigungsstücken von demjenigen, der im gewerblichen Ausmaß das Urheberrecht verletzt. Damit soll dem Rechteinhaber ein besseres Mittel zur Bekämpfung der Produktpiraterie gegeben werden. Es besteht aber nicht nur die Möglichkeit, einen Auskunftsanspruch gegenüber dem Verletzer selbst, sondern nach Abs. 2 auch gegen Dritte durchzusetzen. Dieser soll es dem Rechteinhaber ermöglichen, gegen Verletzer vorzugehen, die für ihn nicht identifizierbar sind, da die für die Identifikation notwendigen Informationen in der Hand des in Anspruch genommenen Dritten liegen. Finden die Rechtsverletzungen im Internet statt, kann z.B. ein Auskunftsanspruch gegen den Host-Provider, der vom Rechtsverletzer öffentlich zugänglich gemachte Inhalte speichert, oder auch den Access-Provider, der den Verletzern Zugang zum Internet ermöglicht, geltend gemacht werden. Wenn eine Auskunft über die Identität des Verletzers nur unter Verwendung von Verkehrsdaten möglich ist, so kann nach Abs. 9 auch über diese Auskunft verlangt werden. Voraussetzung für die Verwendung von Verkehrsdaten ist allerdings eine richterliche Anordnung, die von dem Verletzten beantragt werden muss. Ergeht eine solche richterliche Anordnung, ist der Internet-Provider verpflichtet, die Verkehrsdaten herauszugeben, die eine Identifikation des Verletzers ermöglichen. In vielen Fällen wird der Internet-Provider aber gerade diese Daten bereits gelöscht haben. Denn nach § 96 Abs. 1 S. 3 Telekommunikationsgesetz (TKG) sind Verkehrsdaten in der Regel nach Beendigung der Verbindung unverzüglich zu löschen. Die nach § 113b TKG vorgeschriebene Vorratsdatenspeicherung für Anbieter öffentlich zugänglicher Telekommunikationsdienste wird von der Bundesnetzagentur derzeit nicht durchgesetzt.[1] Oftmals werden aber Verkehrsdaten von den Providern zur Störungsbeseitigung nach § 100 TKG bis zu sieben Tage gespeichert. In der Vergangenheit stellte sich bereits häufiger die Frage, ob Internet-Provider verpflichtet sind, die so gespeicherten Verkehrsdaten länger vorrätig zu halten, wenn sie durch den Urheber auf eine mögliche Rechtsverletzung aufmerksam gemacht wurden. Der BGH nahm nun Stellung zu der Frage, ob der Auskunftsanspruch nach § 101 UrhG auch eine Speicherpflicht des Auskunftsverpflichteten in Bezug auf die für die Auskunft erheblichen Daten beinhaltet.

1 siehe hierzu Baur, Vorerst gescheitert, DFN-Infobrief Recht 10/2017

II. Sachverhalt

In dem Verfahren streiten eine Tonträgerherstellerin als Klägerin und ein Internetprovider als Beklagte. Die Klägerin behauptet, einige Kunden der Beklagten hätten Musikaufnahmen, zu denen die Klägerin die ausschließlichen Verwertungsrechte hat, auf einer Filesharing-Plattform illegal zur Verfügung gestellt. Um mögliche Ansprüche gegenüber diesen Kunden geltend machen zu können, forderte die Klägerin die Beklagte auf, die Verbindungsdaten zu den dynamischen IP-Adressen der Kunden zunächst nicht zu löschen. Die Daten sollten solange gespeichert werden, bis ein Auskunftsverfahren nach § 101 Abs. 2 und Abs. 9 UrhG abgeschlossen ist. Dem kam die Beklagte jedoch nicht nach und löschte die meisten der Verbindungsdaten. Die Klägerin hat nun vor Gericht beantragt, festzustellen, dass die Beklagte verpflichtet gewesen wäre die IP-Adressen in Verbindung mit den jeweiligen Verbindungsdaten (Zeiten, interne Kundenbezeichnung, Kundennummer, Benutzerkennung) bis zur Erteilung der Auskunft zu speichern.

III. Entscheidung des BGH

Neben einigen prozessualen Problemen befasste sich der BGH in dem Verfahren mit der Frage, ob der Rechteinhaber einen Anspruch auf Unterlassung der Löschung von Daten zur Sicherung des Auskunftsanspruchs gegenüber dem Internet-Provider hat, wenn dieser ihm zur Auskunft nach § 101 Abs. 2 Nr. 3 UrhG verpflichtet ist. Er ist der Ansicht, dass, auch wenn es sich dem Wortlaut nach nur um einen Auskunftsanspruch handelt, sich aus § 101 Abs. 2 und Abs. 9 UrhG in Verbindung mit § 96 Abs.1 S. 1 TKG eine Speicherpflicht des Internet-Providers für die Dauer des Gestattungsverfahrens nach § 101 Abs. 9 UrhG ergibt. Durch die Löschpflicht nach § 96 Abs. 1 S. 3 TKG sei der Anwendungsbereich eines solchen Anspruchs von vornherein sehr klein und betreffe sowieso nur die Fälle, in denen der Provider die Daten noch nicht vor Beginn des Gestattungsverfahrens gelöscht habe.

Eine solche Auslegung ergebe sich auch unter Berücksichtigung der unionsrechtlichen Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums, die durch § 101 Abs. 2 UrhG in nationales Recht umgesetzt wurde. Zweck der Richtlinie sei es, dem Inhaber des verletzten Rechts die Möglichkeit einzuräumen, Beweismittel zu sichern, die den Rechtsverletzer identifizieren, damit der Rechteinhaber dann seine Ansprüche ihm gegenüber geltend machen kann. Zu diesem Zweck könne auch Auskunft von einem Internet-Provider verlangt werden, der selbst die Rechtsverletzung nicht begangen hat. Es liefe dem Sinn der Richtlinie entgegen, wenn der Internet-Provider in einem solchen Fall frei entscheiden kann, ob er die benötigten Daten bereits vor Erteilung der Auskunft löscht.

Eine solche Ansicht widerspreche auch nicht der Löschpflicht aus § 96 Abs. 1 S. 3 TKG. Neben den im TKG genannten Gründen dürfen nach § 96 Abs. 1 S. 2 TKG Verkehrsdaten auch für durch andere gesetzliche Vorschriften begründete Zwecke verwendet werden. Eine solche gesetzliche Vorschrift stelle § 101 Abs. 9 UrhG dar. Ermöglicht das TKG die Verwendung der Verkehrsdaten für einen solchen Auskunftsanspruch, könne die Löschpflicht nicht gelten, solange die Daten für den Auskunftsanspruch noch erforderlich seien.

Auch stehen dieser Ansicht nicht die Erwägungen aus dem Urteil des EuGH vom 08.04.2014 (C-293/12 und C-594/12), in dem die Richtlinie über die Vorratsdatenspeicherung aufgehoben wurde, entgegen. Im Gegensatz zur Vorratsdatenspeicherung sei hier der Anwendungsbereich auf den kleinen Bereich offensichtlicher Rechtsverletzungen klar beschränkt und stehe sowohl unter dem Vorbehalt der Verhältnismäßigkeit nach § 101 Abs. 4 UrhG als auch unter dem Richtervorbehalt nach § 101 Abs. 9 UrhG.

IV. Fazit

Auch Hochschulen und Forschungseinrichtungen könnten von dieser Speicherpflicht betroffen sein, wenn Urheber oder andere Rechteinhaber eine Auskunft nach § 101 Abs. 2 Nr. 3 UrhG fordern. Hochschulen bieten Mitarbeitern und Studierenden einen eigenen Internetzugang und erbringen damit Dienstleistungen, die im Sinne des § 101 Abs. 2 Nr. 3 UrhG für rechtsverletzende Tätigkeiten genutzt werden könnten. Dies kann zum Beispiel der Fall sein, wenn Nutzer des Hochschulanschlusses über den Internetzugang Raubkopien verbreiten. Voraussetzung des Auskunftsanspruches nach § 101 Abs. 2 UrhG ist, dass die durch den Dritten erbrachten Dienstleistungen ein gewerbliches Ausmaß erreicht haben. Dieses Kriterium soll sicherstellen, dass nur derjenige mit dem technischen Aufwand eines Auskunftsanspruchs belastet wird, der die Dienstleistung gewerbsmäßig erbringt. Ab wann allerdings von

einem gewerblichen Ausmaß in Absatz 2 gesprochen werden kann, wird im Gesetz nicht näher definiert. Nach der Gesetzesbegründung fallen darunter solche Provider, die zwecks Erlangung eines unmittelbaren oder mittelbaren wirtschaftlichen oder kommerziellen Vorteils handeln. Unabhängig von der Frage, ob Hochschulen und Forschungseinrichtungen unter Umständen auch mittelbare wirtschaftliche Vorteile mit der Erbringung ihrer Dienste bewirken, spricht insbesondere der Umfang der Dienstleistungen dafür, hier von einer Dienstleistung im gewerblichen Ausmaß auszugehen. Da Hochschulen und Forschungseinrichtungen in einem Umfang Dienste erbringen, der mit gewerblichen Anbietern durchaus vergleichbar ist, muss von einer gleichen Einordnung im Hinblick auf § 101 Abs. 2 UrhG ausgegangen werden.

Anders als bei dem Auskunftsanspruch gegenüber dem Verletzer nach § 101 Abs. 1 UrhG setzt der Auskunftsanspruch gegenüber einem Dritten nach Ansicht des BGH (Beschluss vom 19. 4. 2012 - I ZB 80/11) nicht ein gewerbliches Ausmaß der Rechtsverletzung selbst voraus, so dass bereits Einzeltaten einen Auskunftsanspruch auslösen können. Die Grenze eines Auskunftsanspruchs ist dabei allerdings stets die Verhältnismäßigkeit einer solchen Anfrage.

Entstehen den Hochschulen und Forschungseinrichtungen durch die Auskunft Kosten, so können sie diese nach § 101 Abs. 2 S. 3 UrhG von dem Verletzten zurückverlangen. Auch die Kosten der richterlichen Anordnung nach § 101 Abs. 9 UrhG trägt der Antragsteller selbst.

Weiterleiten zur Kündigung

Rechtsprechung zum Arbeitsrecht in Kürze: E-Mail-Weiterleitung als außerordentlicher Kündigungsgrund

von Armin Strobel

Das unbefugte Weiterleiten von dienstlichen E-Mails an eine private E-Mail-Adresse kann eine außerordentliche Kündigung rechtfertigen. Mit seinem Urteil vom 16. Mai 2017 (Az. 7 Sa 38/17) hat das Landesarbeitsgericht (LAG) Berlin-Brandenburg einen weiteren Fall entschieden, in dem es um die Voraussetzungen einer außerordentlichen Kündigung geht. Mitarbeiter von Forschungseinrichtungen sind hiervon ebenso betroffen, wie Arbeitnehmer in der freien Wirtschaft.

I. Hintergrund

Wie bereits in vorherigen Beiträgen des DFN-Infobriefs Recht ausgeführt, stellt die außerordentliche Kündigung ein scharfes Schwert im Arbeitsrecht dar und ist daher an strenge Voraussetzungen geknüpft.[1] Insbesondere muss ein wichtiger Grund im Sinne des § 626 Abs. 1 des Bürgerlichen Gesetzbuchs (BGB) vorliegen. Hierfür muss es aufgrund des kündigungsrelevanten Verhaltens „an sich" – also abstrakt und losgelöst vom konkreten Einzelfall – unzumutbar für den Arbeitgeber sein, das Arbeitsverhältnis zumindest bis zum Ablauf der ordentlichen Kündigungsfrist fortzuführen. Kann diese abstrakte Prüfung bejaht werden, stellt sich anschließend die Frage, ob auch im konkreten Einzelfall Tatsachen vorliegen, aufgrund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der Interessen beider Seiten die Fortsetzung des Arbeitsverhältnisses – und sei es nur bis zum Ende der ordentlichen Kündigungsfrist – zugemutet werden kann.

Diese zentrale Voraussetzung der außerordentlichen Kündigung macht deutlich, dass durch diese arbeitsrechtliche Maßnahme nicht primär ein in der Vergangenheit liegendes Ereignis sanktioniert werden, sondern vielmehr eine Prognoseentscheidung bezüglich der zukünftigen Zusammenarbeit getroffen werden soll. Infolgedessen ist Grundlage einer jeden außerordentlichen Kündigung eine detaillierte Bewertung des Einzelfalls, die nicht generalisiert werden kann. Rechtsprechung in diesem Zusammenhang kann daher lediglich als Orientierungshilfe dienen, eine eigenständige Prüfung des konkreten Falls aber nicht ersetzen.

II. Sachverhalt der Entscheidung

Eine entsprechende Indizwirkung entfaltet auch die Entscheidung des LAG Berlin-Brandenburg. Hintergrund ist ein Rechtsstreit zwischen einem ehemaligen Arbeitnehmer und dessen ehemaligen Arbeitgeber. Der Arbeitnehmer hat kurz vor einem beruflichen Wechsel zu einem direkten Wettbewerber des Arbeitgebers mehrere E-Mails mit dienstlichem Bezug an seine private E-Mail-Adresse weitergeleitet. Darunter waren E-Mails mit Kundeninformationen und solche mit Angebots- und Kalkulationsunterlagen für ein laufendes Projekt des Arbeitgebers.

Der Arbeitnehmer behauptet die E-Mails zum dienstlichen Gebrauch im Rahmen der Heimarbeit zu benötigen, wohingegen der Arbeitgeber vermutet, dass die Informationen für die künftige Beschäftigung im Konkurrenzunternehmen nutzbar gemacht werden sollen. Die genaue Anzahl der weitergeleiteten E-Mails ist dabei umstritten.

1 Zu den Voraussetzungen und weiteren Praxisbeispielen der außerordentlichen Kündigung siehe unter anderem: Heuer, Was zu viel ist, ist zu viel…, DFN-Infobrief Recht 10/2016 und Strobel, Kenne die Grenzen!, DFN-Infobrief Recht 01/2017.

III. Entscheidung des LAG Berlin-Brandenburg

Mit seiner Entscheidung hob das LAG Berlin-Brandenburg im Berufungsverfahren das vorinstanzliche Urteil auf und bejaht die Voraussetzungen der außerordentlichen Kündigung. Insbesondere auf das Vorliegen eines wichtigen Grundes geht das Gericht dabei vertieft ein.

Hierbei stellt es zunächst fest, dass neben der Verletzung einer vertraglichen Hauptpflicht auch die Verletzung einer Nebenpflicht (im Sinne des § 241 Abs. 1 BGB) ein wichtiger Grund für eine fristlose Kündigung „an sich" sein kann. Im Rahmen dieser Nebenpflichten sind die Vertragsparteien dazu verpflichtet auf die Rechte, Rechtsgüter und Interessen der anderen Partei Rücksicht zu nehmen. Vor diesem Hintergrund ist es dem Arbeitnehmer verwehrt, ohne das Einverständnis des Arbeitgebers betriebliche Unterlagen oder Daten zu vervielfältigen oder sich anzueignen. Sind von den Unterlagen und Daten sogar Betriebs- oder Geschäftsgeheimnisse erfasst, kann darüber hinaus eine strafbewehrte Handlung (vergleiche § 17 Abs. 2 Nr. 1b UWG) vorliegen. Verletzt der Arbeitnehmer somit eine vertragliche Nebenpflicht, kann im Rahmen der abstrakten Beurteilung ein wichtiger Grund im Sinne der fristlosen Kündigung zu sehen sein, sodass die unautorisierte E-Mail-Weiterleitung an eine private E-Mail-Adresse die abstrakte Ebene der Prüfung erfüllt.

Auch unter Berücksichtigung des konkreten Falls bejaht das Gericht das Vorliegen eines wichtigen Grunds für eine außerordentliche Kündigung. Im Rahmen einer Gesamtabwägung ist bei dieser Prüfung das Interesse des Arbeitgebers an einer sofortigen Beendigung des Arbeitsverhältnisses gegenüber dem Interesse des Arbeitnehmers an dessen Fortbestand abzuwägen. Hierbei sind regelmäßig das Gewicht und die Auswirkungen der Pflichtverletzung, der Grad des Verschuldens, eine mögliche Wiederholungsgefahr sowie die Dauer des Arbeitsverhältnisses und dessen störungsfreier Verlauf zu berücksichtigen. Das Gericht bewertet damit im Ergebnis das Interesse des Arbeitgebers als schützenswerter gegenüber dem Interesse des Arbeitnehmers.
Es begründet die Entscheidung damit, dass die E-Mails wesentliche Geschäftsinformationen enthielten und für den Arbeitnehmer keine dienstliche Notwendigkeit für die Weiterleitung an die private E-Mail-Adresse bestand, da der Arbeitgeber Arbeitsmittel für die Heimarbeit bereitstellte. Auch der Arbeitsvertrag kann die E-Mail-Weiterleitung nicht rechtfertigen, da eine private Speicherung von Geschäftsinformationen gerade untersagt wurde. Außerdem ist zu berücksichtigen, dass der Arbeitnehmer kurz vor einem Arbeitsplatzwechsel zu einem Wettbewerber des Arbeitgebers stand und die Verhandlungen diesbezüglich schon weit vorangeschritten waren. Dadurch bestand die Gefahr, dass der Arbeitnehmer die in den E-Mails enthaltenen Informationen für seinen neuen Arbeitgeber verwendet. Das geschäftliche Interesse des alten Arbeitgebers ist dadurch in erheblichem Maß beeinträchtigt worden, worauf es nach Ansicht des Gerichts der Arbeitnehmer auch abzielte. Da aufgrund des bevorstehenden Wechsels des Arbeitgebers zu befürchten war, dass der Arbeitnehmer weitere dienstliche Informationen abgreift, war es nach Auffassung des Gerichts dem Arbeitgeber auch nicht zumutbar die ordentliche Kündigungsfrist abzuwarten.

Auch die übrigen Voraussetzungen der außerordentlichen Kündigung bejaht das Gericht. Weder stand dem Arbeitgeber ein milderes Mittel im Vergleich zur fristlosen Kündigung zur Verfügung, noch erfolgte die Beteiligung des Betriebsrats fehlerhaft. Damit ist nach Auffassung des Gerichts die außerordentliche Kündigung rechtmäßig und die Klage des ehemaligen Arbeitnehmers erfolglos.

IV. Fazit und Konsequenzen für Forschungseinrichtungen

Mit seiner Entscheidung hat das LAG Berlin-Brandenburg rechtlich zwar kein Neuland betreten, aber dennoch einen Beitrag zur Rechtssicherheit geleistet. Die grundsätzlichen Voraussetzungen der außerordentlichen Kündigung sind auch im Umfeld von Forschungseinrichtungen bekannt und nicht überraschend. Mithilfe des entschiedenen Falls können Forschungseinrichtungen aber anhand eines neuen Praxisbeispiels prüfen, ob potentiell kündigungsrelevantes Verhalten tatsächlich die Voraussetzungen der arbeitsrechtlichen Sanktionen erfüllt.

Gerade die Weiterleitung von E-Mails im Rahmen des Beschäftigungsverhältnisses spielt immer wieder eine wichtige Rolle im Zusammenhang mit Forschungseinrichtungen. Neben den bekannten datenschutzrechtlichen und strafrechtlichen

Risiken macht die Entscheidung deutlich,[2] dass auch arbeitsrechtliche Konsequenzen – bis hin zur außerordentlichen Kündigung – drohen, wenn die Weiterleitung unautorisiert erfolgt. Eine E-Mail-Weiterleitung an private E-Mail-Adressen sollte daher nicht gedankenlos, sondern gut bedacht erfolgen. Insbesondere sollten die Bestimmungen des Arbeitsvertrags genau geprüft und berücksichtigt werden. Die unautorisierte Weiterleitung von E-Mails kann als (arbeits-)vertragliche Nebenpflichtverletzung nämlich zu drastischen arbeitsrechtlichen Konsequenzen führen. Wie immer bei außerordentlichen Kündigungen gilt es aber die Umstände des konkreten Einzelfalls zu berücksichtigen.

2 Zu der allgemeinen rechtlichen Bewertung von E-Mail-Weiterleitungen im Kontext von Forschungseinrichtungen siehe: Klein, Was lange währt… muss nicht immer gut sein, DFN-Infobrief Recht 06/2015 und Klein, Was lange währt… muss nicht immer gut sein – Teil 2, DFN-Infobrief Recht 07/2015.

Wer hat an der Uhr gedreht?

Statusmeldung zum gegenwärtigen Stand der Umsetzungsgesetze der Länder zur DSGVO

von Charlotte Röttgen

Nachdem der Bund bereits im Sommer 2017 das Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) verabschiedet hat, wartete man in den vergangenen Monaten gespannt auf ein Tätigwerden der Bundesländer. Denn auch sie sind gefragt, ihre Landesdatenschutzgesetze an die Vorgaben der Datenschutz-Grundverordnung (DSGVO) anzupassen. Bei einem Blick in den Kalender stellt man fest: viel Zeit bleibt nicht mehr. Stichtag ist der 25. Mai 2018, der Tag, an dem die DSGVO wirksam werden wird. Dieser Beitrag gibt ausgewählte Einblicke in die unterschiedlichen Gesetzesentwürfe der Länder. Bereichsspezifische Spezialgesetze sind hiervon ausgenommen.

I. Ausgangslage

Vieles ist in den vergangenen Monaten zu der DSGVO und den Neuerungen, die mit ihrem Wirksamwerden einhergehen, geschrieben worden. Ein bisher sparsam behandeltes Thema, das insbesondere auch Forschungseinrichtungen und Hochschulen betrifft, da das Hochschulrecht Angelegenheit der Länder ist, ist das der Umsetzungsgesetze der Länder zu der DSGVO. Diese ist zwar als Verordnung ausgestaltet und gilt daher in allen Mitgliedstaaten der Europäischen Union und somit auch in den Bundesländern unmittelbar, ohne dass es eines weiteren Umsetzungsaktes bedürfte. Allerdings sind in der DSGVO verschiedene Öffnungsklauseln enthalten, welche den nationalen Gesetzgebern in bestimmten Bereichen einen Umsetzungsspielraum belassen.[1] Hierdurch können die Mitgliedstaaten etwa die Verhängung von Geldbußen gegen Behörden und sonstige öffentliche Stellen beschränken bzw. ausschließen oder besondere Ermächtigungsgrundlagen für die Datenverarbeitung der öffentlichen Verwaltung vorsehen. Vielfach bedarf es der Konkretisierung durch Umsetzungsgesetze aber allein deshalb, weil die Normen mit den Öffnungsklauseln sehr allgemein gehalten sind. Die Umsetzungsgesetze dienen also dazu, die Öffnungsklauseln – sofern vom Gesetzgeber gewollt – auszufüllen und landesspezifische Regelungen vorzusehen. Eine bloße Wiederholung des Gesetzeswortlauts der DSGVO ist hierbei jedoch aufgrund des Wiederholungsverbots untersagt. Soweit erforderlich, darf der Wortlaut zu Klarstellungszwecken lediglich in Teilen übernommen werden. Die DSGVO ist nunmehr das maßgebliche Gesetz, die nationalen Datenschutzgesetze dienen als Ergänzung. Daher sind auch strengere Vorgaben, als von der DSGVO vorgesehen, auf mitgliedstaatlicher Ebene nicht zulässig.

Auf Bundesebene hat der Gesetzgeber bereits im Sommer 2017 das Datenschutz-Anpassungs- und Umsetzungsgesetz-EU (DSAnpUG-EU) verabschiedet, welches nun im BDSG-neu enthalten ist.[2] Für die Anpassung der Landesdatenschutzgesetze sind die Bundesländer zuständig. Diese haben seit dem Inkrafttreten der DSGVO im Mai 2016 ihren Gesetzgebungsauftrag recht zögerlich angenommen. Inzwischen existieren zumindest in allen 16 Bundesländern Entwürfe für die neuen, DSGVO-konformen Landesdatenschutzgesetze, verabschiedet sind bisher nur ein paar – viel Zeit bleibt den Landesparlamenten nicht mehr.

1 siehe hierzu Sydow, Vereinheitlichung des EU-Datenschutzrechts?, DFN Infobrief-Recht 05/2016.

2 siehe hierzu Leinemann, Auf die Plätze, fertig, los, DFN Infobrief-Recht 10/2017.

II. Entwicklungen auf Landesebene

Vermutete man bislang, die Länder würden sich gänzlich an dem DSAnpUG-EU des Bundes orientieren, gibt es – ausweislich der Gesetzesentwürfe – zumindest ein paar Überraschungen. Im Folgenden werden exemplarisch einige für Hochschulen und Forschungseinrichtungen relevante Beispiele vorgestellt. Vorweg zu nehmen ist, dass es zu einigen Unterschieden in der datenschutzrechtlichen Ausgestaltung kommen wird und eine einheitliche Betrachtung der Umsetzung einzelner Öffnungsklauseln daher schwer möglich ist.

1. Bußgelder bei Datenschutzverstößen

Der besondere „Anreiz" der DSGVO, datenschutzrechtliche Vorgaben einzuhalten, soll – so die Intention des Unionsgesetzgebers – die Aussicht auf drohende Bußgelder in empfindlicher Höhe sein. Nach Art. 83 DSGVO können bei Datenschutzverstößen Bußgelder in Höhe von bis zu 20.000.000 EUR oder bei Unternehmen von 4 % des weltweit erzielten Jahresumsatzes verhängt werden.

Für öffentliche Stellen gelten diese Vorschriften aber nicht zwingend. In Art. 83 Abs. 7 DSGVO ist eine Öffnungsklauseln enthalten, die es den Mitgliedstaaten überlässt, zu entscheiden, ob und in welchem Maß die Verhängung von Bußgeldern gegenüber öffentlichen Stellen möglich sein soll. Der Bundesgesetzgeber hat von dieser Öffnungsklausel Gebrauch gemacht. Gem. § 43 Abs. 3 BDSG-neu werden grundsätzlich keine Bußgelder gegen Behörden und sonstige öffentliche Stellen verhängt. Eine Ausnahme besteht gem. § 2 Abs. 5 BDSG-neu allerdings dann, wenn eine öffentliche Stelle als öffentlich-rechtliches Unternehmen am Wettbewerb teilnimmt. In diesem Fall gilt die eigentlich öffentliche als nichtöffentliche Stelle i.S.d. Datenschutzrechts und die Bußgeldvorschriften sind anwendbar.

Wie sich nun abzeichnet, sind die Landesgesetzgeber dieser Lösung gefolgt. Die neuen Entwürfe aller Landesdatenschutzgesetze sehen eine grundsätzliche Bereichsausnahme für Behörden und sonstige öffentliche Stellen für die Verhängung von Bußgeldern vor, es sei denn, diese stehen mit anderen Unternehmen im Wettbewerb (s. etwa Art. 23 Abs. 3 und Art. 22 des Entwurfs des Bayerischen Datenschutzgesetzes (BayDSG-E), § 24 Abs. 2 und § 2 Abs. 3 des Entwurs des Hamburgischen Datenschutzgesetzes (HmbDSG-E) sowie § 20 Abs. 4 des Entwurfs des Niedersächsischen Datenschutzgesetzes (NDSG-E)). Diese Umsetzung ist nach dem Gleichbehandlungsgebot wenig verwunderlich, da der Staat sich nicht auf Privilegien stützen darf, wenn er als Wettbewerber auftritt.

Ob in der Praxis immer eindeutig auszumachen sein wird, wann eine öffentlich-rechtliches Unternehmen die Verarbeitung personenbezogener Daten zu wirtschaftlichen Zwecken vornimmt und daher mit anderen Unternehmen im Wettbewerb steht, darf bezweifelt werden. Im Bereich des öffentlichen Rechts ist die Verhängung von Bußgeldern aber nach neuem Datenschutzgesetz auf Bundes- und Landesebene ausgeschlossen.

2. Zweckänderung zu Forschungszwecken, Art. 5 Ib, 89 I DSGVO

Ein weiterer Aspekt, der für Hochschulen und Forschungseinrichtungen relevant ist, stellt die mögliche Zweckänderung bei der Datenverarbeitung zu Forschungszwecken dar.[3] Hierbei handelt es sich um eine Lockerung vom sog. Zweckbindungsgrundsatz, der besagt, dass personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Nach Art. 5 Abs. 1 lit. b i.V.m. Art. 89 Abs. 1 DSGVO gilt eine Weiterverarbeitung der Daten zu anderen Zwecken als mit dem Ursprungszweck vereinbar, wenn die Weiterverarbeitung der personenbezogenen Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erfolgt.

Die Landesgesetzgeber haben hier von dem Spielraum, den die Öffnungsklausel in Art. 6 Abs. 4 DSGVO vorsieht, Gebrauch gemacht und sehen teilweise deutliche Einschränkungen vor. Nach § 8 Abs. 2 Nr. 7 DSG NRW-E ist eine Verarbeitung personenbezogener Daten zu anderen Zwecken, als zu jenen, zu denen sie ursprünglich erhoben worden sind, zulässig, wenn sie zur Durchführung wissenschaftlicher oder historischer Forschung erforderlich ist, das wissenschaftliche oder histo-

3 Zu der DSGVO im Kontext wissenschaftlicher Beschäftigungsverhältnisse Röttgen, Was kommt, was geht, was bleibt, DFN Infobrief-Recht 10/2017.

rische Interesse an der Durchführung des Forschungsvorhabens das Interesse der betroffenen Person an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck auf andere Weise nicht oder nur unter unverhältnismäßigem Aufwand erreicht werden kann, Art. 6 Abs. 2 Nr. 3c BayDSG-E.

3. Auskunftsrecht, Art. 15 DSGVO

Ein weiteres Charakteristikum der DSGVO ist die Stärkung der Betroffenenrechte, wie etwa das Auskunftsrecht nach Art. 15 DSGVO. Hiernach steht dem von einer Verarbeitung seiner personenbezogenen Daten Betroffenen ein Recht auf Auskunft gegenüber der verantwortlichen Stelle zu. Der Betroffene ist auf dessen Anfrage umfangreich über Art und Ausmaß der ihn betreffenden verarbeiteten Daten zu informieren. Dieses Recht gilt allerdings nicht unbeschränkt; Art. 23 Abs. 1 DSGVO sieht Einschränkungsmöglichkeiten zugunsten der Mitgliedstaaten unter bestimmten Bedingungen vor. Von dieser Öffnungsklausel haben nun die Landesgesetzgeber Gebrauch gemacht. Nach § 9 Abs. 2 des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Daten (LDSG) steht dem Betroffenen ein Auskunftsrecht nicht zu, wenn die ihn betreffenden personenbezogenen Daten ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle verarbeitet werden und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie deren Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. Es ist anzumerken, dass die Landesgesetzgeber, die sich für diese Umsetzung entschieden haben, auf einer Linie mit dem Bundesgesetz sind (vgl. § 34 Abs. 1 Nr. 2 lit. b BDSG-neu).

Eine Besonderheit stellt § 11 Abs. 1 DSG NRW-E dar, der für den Fall, dass der Verantwortliche große Mengen personenbezogener Daten des Betroffenen verarbeitet, eine Kooperationspflicht des Betroffenen vorsieht. Der Verantwortliche kann von der betroffenen Person verlangen, die Informationen und Verarbeitungsvorgänge zu präzisieren, auf welche sich das Auskunftsverlangen bezieht. Diese Einschränkung soll dem Erhalt der behördlichen Funktionsfähigkeit i.S.e. Ausuferungsschutzes dienen.

III. Zusammenfassung und Ausblick für die Hochschulen und Forschungseinrichtungen

Die oben dargestellten Stichproben der Umsetzungsgesetze zeigen auf, dass das Datenschutzrecht auf Bundes- und Länderebene zumindest in einigen Punkten einen gesetzgeberischen Gleichklang aufweist. In der Praxis ist aber Vorsicht geboten, da im Einzelnen deutliche Unterschiede bestehen können. Im Vergleich der verschiedenen Umsetzungsgesetze haben die Landesgesetzgeber eigene Akzente gesetzt.

Für die Hochschulen und Forschungseinrichtungen lässt sich Folgendes festhalten: Mit Wirksamwerden der DSGVO und den angepassten Landesdatenschutzgesetzen wird sich keine vollumfänglich einheitliche, länderübergreifende Datenschutzpraxis abzeichnen. Landesspezifische Besonderheiten werden, je nachdem, welches Landesdatenschutzgesetz einschlägig ist, zu unterschiedlichen Bewertungen führen. Eine einheitliche Bewertung wird – voraussichtlich – bei einem der zentralen Themen für Hochschulen und Forschungseinrichtungen möglich sein: die Bereichsausnahme für die Bußgeldtatbestände für Behörden und sonstige öffentliche Stellen. Nur wenn die Verarbeitung personenbezogener Daten als öffentlich-rechtliches Unternehmen erfolgt, das mit anderen im Wettbewerb steht, können im Falle von Datenschutzverstößen Bußgelder verhängt werden. Soweit staatliche Hochschulen und Forschungseinrichtungen öffentlich-rechtlich organisiert sind, unterfallen sie somit in der Regel der privilegierenden Bereichsausnahme. Abweichungen im Einzelfall sind aber möglich, insbesondere wenn es sich bei den Forschungseinrichtungen um solche in privater Trägerschaft handelt. Ob eine Weiterverarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken zulässig ist, muss nach dem jeweiligen Landesrecht beurteilt werden. Wie das Beispiel zeigt, kann es hier durch die Wahrnehmung der Öffnungsklausel zu deutlichen Abweichungen von den Vorgaben der DSGVO kommen. Selbiges gilt für eine etwaige Beschränkung des Auskunftsrechts betroffener Personen.

In den letzten Wochen mehren sich die Nachrichten, dass die Landesparlamente ihre Umsetzungsgesetze verabschieden und für den Stichtag gewappnet sind, ab dem die neue Rechtslage Geltung haben wird. Mit Wirksamwerden der DSGVO verdrängt diese die bisherigen Landesdatenschutzgesetze und gilt auch auf Landesebene unmittelbar. Ausnahmen etwa von den Bußgeldtatbeständen für öffentliche Stellen gibt es in diesem Fall nicht.

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