DFN
infobrief recht

1/2022
Januar 2022

Doppelt lehrt besser
Zur datenschutzrechtlichen Relevanz von Hybridveranstaltungen

Ein Tool, die Banner zu knechten
Mit dem Inkrafttreten des Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) ändern sich die Vorschriften für die Einholung von Einwilligungen für Cookies auf Webseiten

In geheimer Mission
Ein forschungsspezifischer Überblick über das Geschäftsgeheimnisrecht

Doppelt lehrt besser

Zur datenschutzrechtlichen Relevanz von Hybridveranstaltungen

von Owen Mc Grath

Mit der langsamen und teilweisen Rückkehr des Lehrbetriebes in die Präsenz treten neue Konzepte auf den Plan. So werden an vielen Universitäten Vorlesungen und andere Veranstaltungen als Hybride zwischen digitaler Lehre und Präsenzlehre angeboten. Der unter Berücksichtigung der Hygienemaßnahmen nur in Teilen besetzte Hörsaal oder Seminarraum wird hierzu gefilmt und für Studierende daheim online live gestreamt. Teilweise werden die Vorlesungen für den späteren Konsum auch aufgezeichnet. Dieses Vorgehen ermöglicht eine teilweise Rückkehr zu den Lehrbedingungen vor der Pandemie und gleichzeitig eine Berücksichtigung der nach wie vor bestehenden Ansteckungsgefahr. Während die datenschutzrechtlichen Probleme digitaler Veranstaltungen bereits öfter Thema des Infobriefs Recht[1] waren, sind die Fallstricke der Hybridveranstaltungen noch nicht beleuchtet worden.

I. Datenschutzrechtliche Problemstellung

Hybride sowie rein digitale Veranstaltungen weisen einen großen Überschneidungsbereich in Bezug auf ihre rechtlichen Probleme auf. In beiden Modi stellt sich die Frage, inwiefern personenbezogene Daten von digitalen Teilnehmenden verarbeitet werden und ob dies gerechtfertigt ist. Auch wenn der Schluss naheliegt, dass sich so eine deckungsgleiche Bewertung der beiden Veranstaltungstypen ergibt, ist dies nicht vollständig der Fall. Die Situation der Teilnehmenden, die digital über ein Endgerät der Veranstaltung zugeschaltet sind, ist in weiten Teilen mit der Situation der rein digitalen Lehre vergleichbar. Für die Zwecke dieser Erarbeitungen wird sich daher auf die Verarbeitungen personenbezogener Daten der in Präsenz Teilnehmenden und insofern von der digitalen Situation abweichenden Konstellation beschränkt.

Personenbezogene Daten sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“ (Art. 4 Nr. 1 Datenschutz-Grundverordnung [DSGVO]). Umfasst von diesen Daten sind also auch Bild- oder Tonaufnahmen einer Person. Werden diese verarbeitet, ist der Schutzbereich der DSGVO eröffnet. Der Eingriff in diesen Schutzbereich muss gerechtfertigt sein. Im europäischen Datenschutzrecht gibt es zur Rechtfertigung von Verarbeitungen personenbezogener Daten verschiedene Erlaubnistatbestände. Die Verarbeitung kann zum Beispiel durch ihre Notwendigkeit zur Erfüllung einer vertraglichen Pflicht erforderlich sein. Damit wäre eine Verarbeitung nach Art. 6 Abs. 1 S. 1 lit. b DSGVO rechtmäßig.

Um eine datenschutzrechtliche Einschätzung zu Hybridveranstaltung geben zu können, ist festzustellen, inwiefern personenbezogene Daten in diesem Kontext verarbeitet werden können. Von großer Relevanz ist insofern die Aufnahme der Teilnehmenden via Videokamera und Mikrofon während der Veranstaltung sowie die Wiedergabe von Bild und Ton in

1 Siehe. z.B.: John, Corona is calling, DFN-Infobrief Recht Sonderausgabe Covid-19/2020.

einem Livestream bzw. die Speicherung der Aufnahmen und Zurverfügungstellung an Dritte. Werden hierbei nicht nur der Vortragende sondern auch Teilnehmende gezeigt, können auch deren personenbezogene Daten betroffen sein.

II. Fallgruppen

Vorliegend ist zur Veranschaulichung zwischen mehreren Fallgruppen zu unterscheiden:
1. Es wird nur der Vortragende gestreamt und ggf. aufgezeichnet. Die sonstigen Teilnehmenden der Veranstaltung sind auf dem Bild nicht wahrzunehmen. Auch die Stimmen der Teilnehmenden sind nicht zu hören. Insofern sind die einzig relevanten personenbezogenen Daten die des Vortragenden.

2. Der Vortragende ist zu sehen und zu hören. Die Teilnehmenden der Veranstaltung sind vereinzelt im Bild zu sehen. Dies kann durch Schnittbilder geschehen, die das Publikum aus verschiedenen Blickwinkeln zeigen oder durch Aufnahmen des Vortragenden, in denen auch Teilnehmende (bspw. deren Rücken) zu sehen sind. Nunmehr werden auch personenbezogene Daten der Teilnehmenden verarbeitet. Diese Verarbeitung wiegt umso stärker, wenn die Veranstaltung nicht bloß live gestreamt wird, sondern auch nachträglich in aufgezeichneter Form zugänglich ist. Gleiches gilt dann, wenn der Stream oder die Aufzeichnung nicht nur einem beschränkten Personenkreis, sondern der Öffentlichkeit zugänglich ist.

3. Der Vortragende ist zu sehen und zu hören. Die Teilnehmenden sind explizit im Bild zu sehen und auch ihre Stimmen sind zu hören. Dieser Fall liegt zum Beispiel dann vor, wenn die Veranstaltung interaktiv ausgerichtet ist und Mikrofon und Kamera eingesetzt werden, um Fragen oder Beiträge der Teilnehmenden aufzunehmen. Hierbei werden diverse personenbezogene Daten aller beschriebenen Personen verarbeitet.

Um die Verarbeitung personenbezogener Daten zu rechtfertigen, müsste ein entsprechender Tatbestand des Art. 6 Abs. 1 S. 1 DSGVO erfüllt sein. In Frage kommt für die vorliegenden Sachverhalte sowohl eine Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO, als auch eine Aufgabenausführung im öffentlichen Interesse nach Art. 6 Abs. 1 S. 1 lit. e DSGVO.
Die Einwilligung des Vortragenden zur Aufnahme seiner Person in Bild und Ton einmal vorausgesetzt, stellt sich nur für die Fallgruppen 2 und 3 die Frage, ob eine Rechtfertigung vorliegt.

III. Zur Einwilligung

Eine Einwilligung kann nur dann wirksam erteilt werden, wenn die Anforderungen der Art. 4 Nr. 11 DSGVO und Art. 7 DSGVO erfüllt sind. Dafür muss die Einwilligung unmissverständlich, in informierter Weise und vor allem freiwillig abgegeben worden sein. Freiwillig kann eine Einwilligung nur sein, wenn den Betroffenen durch die Verweigerung der Einwilligung kein wesentlicher Nachteil trifft. Ein solcher läge zum Beispiel vor, wenn durch Verweigerung der Einwilligung die Teilnahme an einer Veranstaltung versagt wird.

Im Rahmen hybrider Veranstaltungen ließe sich argumentieren, dass es den Besuchern der Fallgruppe 2 und 3 durch die Verweigerung der Einwilligung zu der entsprechenden Verarbeitung personenbezogener Daten nicht möglich ist an der Veranstaltung teilzunehmen. Damit würde sie ein wesentlicher Nachteil treffen. Dabei wird allerdings verkannt, dass gerade der Vorteil von Hybridveranstaltungen in der Möglichkeit der Teilnahme auf digitalem Wege liegt. Zwar kommt es, je nach Ausgestaltung der digitalen Zugänglichkeit, auch hierbei zur Verarbeitung personenbezogener Daten (IP-Adressen, Namen der Teilnehmenden). Diese ist aber zum einen nicht zwingend und zum anderen regelmäßig weniger eingriffsintensiv, wenn man sie mit dem Abfilmen der Gesichter und der Aufnahme der Stimme vergleicht. Nicht zwingend ist die Verarbeitung in diesem Kontext, wenn die Teilnahme an dem Stream der Veranstaltung oder das Ansehen der Aufzeichnung technisch so ausgestaltet ist, dass keine personenbezogenen Daten verarbeitet werden. Ein wesentlicher Nachteil besteht mit Ablehnung der Verarbeitung bei hybriden Veranstaltungen, wie sie Fallgruppe 2 und 3 widerspiegeln, damit nicht zwangsläufig.

Ein wesentlicher Nachteil könnte jedoch noch dadurch entstehen, dass den Betroffenen durch die Verweisung auf die digitale Variante der Hybridveranstaltung eine aktive Teilnahme mit Fragen und Wortbeiträgen nicht möglich ist. Ob das der Fall ist, hängt von vielen Unbekannten im Einzelfall ab und lässt sich damit nur schwerlich pauschal einordnen. So hängt es schon von der Veranstaltung als solche ab, ob eine aktive Teilnahme erforderlich ist, bzw. die Unmöglichkeit dieser tatsächlich einen wesentlichen Nachteil bedeutet. Vortragsveranstaltungen zum Beispiel leben nicht zwangsläufig von einem Austausch zwischen Publikum und Referenten. Für Seminare hingegen ist ein Austausch essentiell. Des Weiteren kann der digitale Teil der Veranstaltung auch so ausgestaltet sein, dass

eine aktive Teilnahme möglich ist. Das ist zum Beispiel dann der Fall, wenn Fragen über ein Chatfenster oder ähnliches gestellt werden können. Auch hierbei kann es dann zu Verarbeitungen personenbezogener Daten kommen. Diese werden aber, wie dargelegt, je nach technischer Ausgestaltung, einen geringeren Einschnitt für die Betroffenen bedeuten.

Nach diesen Ausführungen wäre eine mangelnde Freiwilligkeit der Einwilligung nur in bestimmten Fällen anzunehmen. Ein solcher läge zum Beispiel vor, wenn eine Präsenzveranstaltung der Fallgruppe 3 vorliegt, welche eine aktive Teilnahme unbedingt erfordert und der digitale Zugang zu dieser Veranstaltung keine Interaktion ermöglicht. Lehnt der Betroffene Aufnahmen seiner Person ab, ist ihm eine Teilnahme in Präsenz nicht möglich. Die digitale Variante bietet keine vergleichbare Alternative. Mit Versagung der Einwilligung liegt ein wesentlicher Nachteil vor. Die Einwilligung kann mithin nicht freiwillig abgegeben werden.

Abseits solcher oder vergleichbarer Situationen ist jedoch von der Möglichkeit einer freiwilligen Einwilligung auszugehen. Hierbei sind die Voraussetzungen einer wirksamen Einwilligung im Sinne der DSGVO zu beachten (Art. 7 DSGVO). Insbesondere ist bei einer Aufzeichnung und Zurverfügungstellung im Internet der Veranstaltung auch darauf zu achten, hierfür eine Einwilligung einzuholen.

IV. Zur Aufgabenausführung im öffentlichen Interesse

Die Verarbeitung von personenbezogenen Daten ist auch zulässig, wenn „die Verarbeitung […] für die Wahrnehmung einer Aufgabe erforderlich [ist], die im öffentlichen Interesse liegt“ (Art. 6 Abs. 1 S. 1 lit. e DSGVO). Die Durchführung der Lehre an Hochschulen und wissenschaftlichen Einrichtungen ist dem öffentlichen Interesse zuzuordnen. Problematisch ist allerdings, dass es nach Art. 6 Abs. 3 DSGVO für Art. 6 Abs. 1 S. 1 lit. e DSGVO einer geschriebenen Rechtsgrundlage bedarf. Bei Art. 6 Abs. 3 DSGVO handelt es sich um eine sogenannte Öffnungsklausel. Mit solchen soll dem Gesetzgeber ermöglicht werden, bestimmte Sachverhalte durch konkretisierte Normen selber näher zu regeln. Soweit ersichtlich liegt für Hybridveranstaltungen allerdings noch keine die Rechtsgrundlage des Art. 6 Abs. 1 S. 1 lit. e DSGVO spezifizierende Norm vor. Soweit ist eine Verarbeitung personenbezogener Daten auch nicht auf diesen Erlaubnistatbestand zu stützen. Werden solche Regelungen beispielsweise im Rahmen des Satzungsrechtes der Hochschule getroffen, ist darauf zu achten, dass sie im Lichte der verarbeitenden Daten verhältnismäßig ist. Insofern wäre schon in Frage zu stellen, ob das Aufnehmen von Bild und Ton der Teilnehmenden für die Veranstaltung überhaupt erforderlich ist.

Bis eine entsprechende Regelung getroffen wurde, steht Art. 6 Abs. 1 S. 1 lit. e DSGVO allerdings nicht als tauglicher Erlaubnistatbestand zur Verfügung.

V. Fazit

Die Durchführung von Hybridveranstaltung wird mit Fortschreiten der Pandemie ein relevanter Modus Operandi. Je nach technischer Ausgestaltung werden neben den personenbezogenen Daten der Vortragenden auch die der Teilnehmenden verarbeitet. Eine Rechtfertigung dieser Verarbeitung ist im Einzelfall und je nach dem digitalen Parallelangebot über eine Einwilligung der Betroffenen möglich.
Eine pauschale Einschätzung verbietet sich jedoch. Diese birgt immer das Risiko eines Verstoßes gegen das europäische Datenschutzrecht.

Ein Tool, die Banner zu knechten

Mit dem Inkrafttreten des Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) ändern sich die Vorschriften für die Einholung von Einwilligungen für Cookies auf Webseiten

von Nicolas John

Nachdem das TTDSG als neues nationales Datenschutzgesetz seit Dezember die Voraussetzungen für die Einwilligung von Nutzern der sogenannten „Cookies“ auf Webseiten regelt, stellt sich die Frage, ob und was sich nun geändert hat. Auf den ersten Blick scheint das TTDSG neue Möglichkeiten zu bieten, welche das Chaos der Cookie-Banner auf den Webseiten unterbinden können. Doch der zweite Blick zeigt: es ist noch ein langer Weg dorthin.

I. Das neue TTDSG

Am 1. Dezember 2021 ist das neue TTDSG in Kraft getreten. Ziel des Gesetzgebungsverfahrens war es, mehr Rechtssicherheit und Rechtsklarheit im Datenschutzrecht zu schaffen und die Datenschutzvorschriften des alten Telekommunikationsgesetzes (TKG) und Telemediengesetzes (TMG) übersichtlich zusammenzuführen.[1] Außerdem stellt das TTDSG die Umsetzung der ePrivacy-Richtlinie[2] sowie der Cookie-Richtlinie[3] dar. Bisher war die Umsetzung der Richtlinien im TMG nach Ansicht des Europäischen Gerichtshofs (EuGH) nicht ausreichend erfolgt,[4] weshalb der Bundesgerichtshof (BGH) letztendlich in einer Entscheidung[5] eine richtlinienkonforme Auslegung des TMG vornahm.

II. Was sind Cookies?

Als Cookies werden kleine Textdateien bezeichnet, die lokal auf dem Computer des Nutzenden beim Besuch einer Webseite gespeichert werden. Diese Dateien speichern bestimmte Einstellungen oder Informationen zu dem Nutzenden. Die gespeicherten Informationen dienen den Webseitenbetreibenden dazu, den Nutzenden bei einem erneuten Besuch der Webseite wiederzuerkennen und bestimmte Funktionen an diesen anzupassen.

Cookies können dabei unterschiedliche technische Ziele verfolgen. Die Benennung dieser Cookies variiert teilweise, doch stehen hinter den Bezeichnungen die gleichen technischen Absichten. Die sogenannten notwendigen bzw. essentiellen Cookies werden für den Webseitenbesuch zwingend benötigt. Darunter fällt zum Beispiel die Speicherung des Inhalts von Warenkörben. Der Inhalt wird durch das entsprechend gesetzte Cookie nicht „vergessen“, wenn der Nutzende sein Browserfenster schließt.

Performance bzw. technische Cookies speichern dagegen die vom Nutzenden vorgenommenen Einstellungen auf der Webseite. Beim nächsten Besuch können durch diese Cookies die Einstellungen wiederhergestellt werden, ohne dass sie vom Nutzenden jedes Mal erneut vorgenommen werden müssen. Darüber hinaus lassen sie auch Analysen über die Besuche der einzelnen Unterseiten, die Reihenfolge der besuchten Seiten oder den Standort des Nutzenden zu.

Davon zu unterscheiden sind Tracking-Cookies, welche durch die Verknüpfung von Analysedaten mit der IP-Adresse des Nutzenden eine eindeutige Zuordnung möglich machen und sogar webseitenübergreifend an Dritte weitergegeben werden können. Diese Analysen können auch für Marketingzwe-

1 Vertiefend hierzu: John, TTDSG – Die Profis in spe, DFN-Infobrief Recht 5/2021.
2 Richtlinie 2002/58/EG.
3 Richtlinie 2009/136/EG.
4 Zum Urteil des EuGH: Baur, Noch viel zu knabbern, DFN-Infobrief Recht 12/2019.
5 BGH, Urteil v. 28.05.2020, Az. I ZR 7/16.

cke verwendet werden. Dies ist insbesondere der Fall, wenn Unternehmen daran interessiert sind, welche Webseiten von dem Nutzenden der Seite zuvor schon besucht worden waren. Für Werbezwecke gibt es zudem noch sogenannte Werbe- bzw. Marketing-Cookies. Diese dienen Werbetreibenden dazu, bestimmte Suchen des Nutzenden zu speichern und mit hierauf abgestimmten Werbeanzeigen zu reagieren. Auch diese Informationen können mit Dritten geteilt werden, wodurch die Interessen den Nutzenden webseitenübergreifend genutzt und zugeschnittene Anzeigen auf verschiedenen Webseiten oder Geräten angezeigt werden können.

III. Die Einwilligung

Jede Person, die im Internet surft, kennt sie: die Einwilligungsbanner zur Einholung der Erlaubnis des Besuchenden, bestimmte Cookies im Zusammenhang mit der Nutzung der Webseite speichern zu dürfen. Manche Banner sind übersichtlich gestaltet und bieten neben „Alle akzeptieren" auch die Optionen „Nur Notwendige" oder „Individuell" an. Andere Banner wiederum verschleiern die Optionen und versuchen durch Farbe und Schriftgröße Nutzende in alle Cookies einwilligen zu lassen. Oftmals klickt der oder die Nutzende genervt auf „Alle akzeptieren", um schnellstmöglich zum eigentlichen Inhalt der Webseite zu gelangen.

Grund für diese sehr unterschiedlichen Ausgestaltungen der Cookie-Banner sind die wenigen Vorschriften an die Ausgestaltung der Banner. Der BGH[6] stellte unter richtlinienkonformer Auslegung des in seiner damaligen Fassung geltenden TMGs fest, dass für die Verwendung von technisch nicht erforderlichen Cookies der Webseitenbetreibende eine aktive Zustimmung des Nutzenden einholen muss (Opt-In). Vorausgewählte Kästchen (Opt-Out) genügen den Anforderungen der Einwilligung nicht. Weitere Vorgaben existierten nicht.
Diese Auslegung manifestiert der Gesetzgeber nun in § 25 TTDSG ausdrücklich. Danach muss der Nutzende einer Webseite bei der Verwendung von Cookies oder ähnlichen Technologien „auf der Grundlage von klaren und umfassenden Informationen" einwilligen. Für die Ausgestaltung der Informationen und Einwilligung verweist das TTDSG auf die Vorschriften der Datenschutz-Grundverordnung (DSGVO).[7]

Die Einwilligung muss ausnahmsweise nicht erteilt werden, wenn die Speicherung unbedingt erforderlich ist, um den vom Nutzenden ausdrücklich gewünschten Dienst überhaupt bereitstellen zu können. Dies entspricht in jedem Fall den essentiellen Cookies, wie beispielsweise der Speicherung des Warenkorbs oder der Login Daten. Welche Cookies darüber hinaus aber unter die Einwilligungspflicht fallen, legt das TTDSG nicht fest. Insbesondere bei technischen Cookies kann die Grenze zwischen Erforderlichkeit für den „ausdrücklich gewünschten Telemediendienst" und der Einwilligungspflicht schnell verschwimmen. Auch nicht genauer geregelt wird die Ausgestaltung der Cookie-Banner. Insoweit wird den Webseitenbetreibenden weiterhin ein weiter Spielraum gelassen.

IV. Personal Information Management System

Durch die neugeschaffene Regelung des § 25 TTDSG ändert sich zunächst nichts an der bisherigen Praxis. Die Erforderlichkeit der Einwilligung wird normativ festgelegt, ein Ende der Cookie-Banner wird dadurch nicht geschaffen. Doch die Abhilfe könnte durch die Regelungen des § 26 TTDSG erfolgen. Dieser erlaubt die Verwendung von sogenannten „Personal Information Management Systems", kurz PIMS.

1. Was sind PIMS?

PIMS sind Systeme, die den Nutzenden die Möglichkeit geben sollen, mehr Kontrolle über ihre persönlichen Daten zu haben. In Bezug auf Cookies könnte dies dadurch stattfinden, dass mit Hilfe von PIMS die Nutzenden vorab festlegen können, in welche Nutzung von Cookies eingewilligt wird und in welche nicht. Der Vorteil hieraus besteht darin, dass der einzelne Webseitenbetreibende nicht mehr mit einem Banner die Präferenzen des Nutzenden abfragen muss, sondern anhand des PIMS diese Information direkt erhält.

Außerdem soll das PIMS durch einen Drittanbietenden verwaltet werden. Dieser soll kein Eigeninteresse an der Erteilung der Einwilligung und den verwalteten Daten haben und unabhängig von Unternehmen sein, die ein solches Interesse haben können. Dadurch kann die nutzende Person eine differenzierte Entscheidung über die einzelnen Cookies und ihre Zwecke treffen, ohne durch Farbe und Schriftgröße zu einer

6 BGH, Urteil v. 28.05.2020, „Cookie Einwilligung II", Az.: I ZR 7/16.
7 Zur datenschutzrechtlichen Einwilligung siehe Fischer, Ja, ich will!, DFN-Infobrief Recht 03/2020.

Einwilligung beeinflusst zu werden, die sie nicht möchte. Zum Beispiel kann auf diese Weise bestimmten Tracking-Cookies zugestimmt werden, aber die Nutzung von Werbe-Cookies von ausgewählten Unternehmen unterbunden werden.

2. Anerkennungsverfahren für PIMS-Dienstanbietende

Doch zum jetzigen Zeitpunkt ist die Verwendung eines PIMS nur Theorie. Denn das TTDSG normiert nur ein Anerkennungsverfahren für Anbietende eines PIMS-Dienstes. Danach ist es möglich, dass Anbietende von PIMS, welche bestimmte Bedingungen erfüllen, von einer unabhängigen Stelle anerkannt werden. Die Voraussetzungen dieses Anerkennungsverfahrens müssen zuvor aber in einer Rechtsverordnung durch die Bundesregierung festgelegt werden. Für eine flächendeckende Anwendung der PIMS in der Praxis ist es demnach im nächsten Schritt erforderlich, dass die Bundesregierung eine Verordnung schafft, welche die Anforderungen an einen solchen Dienst festlegt. Wann diese kommt, bleibt vorerst offen.

3. Praxisprobleme mit PIMS

Darüber hinaus stellen sich weitere Probleme in der Praxis. Einerseits sind Browserherstellende verpflichtet, die Cookie-Einstellungen der Nutzenden über die Browservoreinstellungen zu beachten, andererseits müssen sie die PIMS-Einstellungen umsetzen. Sollten sich die Einstellungen widersprechen, ist erstmal unklar, welche Einstellungen Vorrang genießen. Der Wortlaut des TTDSG lässt vermuten, dass die Browsereinstellungen vorrangig sind, doch führt das Gesetz das Verhältnis nicht genauer aus.

Aber auch Webseitenbetreibende müssen sich mit den PIMS nun umfassend auseinandersetzen: Nicht nur, dass Schnittstellen geschaffen werden müssen, um Einstellungen von PIMS berücksichtigen zu können und auf der eigenen Webseite umzusetzen. Es zeigt sich auch, dass das TTDSG davon ausgeht, dass eine individuelle Einwilligung des Nutzenden auf der Webseite weiterhin Vorrang gegenüber den PIMS-Einstellungen haben soll. Für Webseitenbetreibende bleibt damit die Möglichkeit, weiterhin nach einer individuellen Einwilligung in bestimmte Cookies zu fragen, wenn eine Einwilligung über das PIMS nicht vorher schon erteilt wurde. Die Hoffnung, dass Cookie-Banner der Vergangenheit angehören werden, ist daher eher kritisch zu betrachten. Es ist vielmehr zu befürchten, dass die Einwilligungsbanner auf den Webseiten trotz des Einwilligungsmanagements der Nutzenden nicht wesentlich abnehmen werden.

Außerdem offenbart sich ein weiteres Defizit des TTDSG. Während die Missachtung von Einwilligungen der Nutzenden in Cookies nach § 25 TTDSG mit Geldbußen bis zu 300.000 Euro von den Aufsichtsbehörden sanktioniert werden kann, sieht das Gesetz keine entsprechende Regelung für die Missachtung von Einwilligungen, welche mittels PIMS getroffen wurden. Telemedien-Anbietende können damit PIMS-Einstellungen ignorieren, ohne Sanktionen befürchten zu müssen.

V. Fazit für Hochschulen und Forschungseinrichtungen

Für Hochschulen und Forschungseinrichtungen als Webseitenbetreibende ändert sich mit dem neuen TTDSG zunächst wenig. Die Einwilligungen der Nutzenden in technisch nicht erforderliche Cookies müssen weiterhin eingeholt werden. In der Abgrenzungsfrage, bei welcher Art von Cookie die Einwilligung erforderlich ist, gibt das TTDSG weiterhin keine genaueren Kategorien zur Hand. Insoweit bleibt zu empfehlen im Zweifelsfall die Einwilligung zu kritischen Cookies einzuholen. Bezüglich der Ausgestaltung des Cookie-Banners schreibt das TTDSG nun das Opt-In-Verfahren ausdrücklich vor, um eine Einwilligung des Nutzenden wirksam einzuholen. Da dies dem aktuellen Stand der Rechtsprechung entspricht, sollte an dieser Stelle nicht nachgebessert werden müssen.

Sobald die erforderliche Rechtsverordnung für die Einwilligung unter Zuhilfenahme von PIMS von der Bundesregierung erlassen wird, müssen die Webseiten der Hochschulen und Forschungseinrichtungen auch daran angepasst werden.

Insgesamt sind die Vorschriften zum Cookie-Management nur teils gelungen. Zwar werden durch die neuen Normen unanwendbare Vorschriften und damit verbundene Unsicherheiten beseitigt und die aktuelle Rechtsprechung zur Einholung von Einwilligungen in die Nutzung von Cookies manifestiert, doch bleiben weiterhin Fragen bezüglich der Erforderlichkeit einer Einwilligung offen. Die Möglichkeit der Verwendung von PIMS ist zunächst ein Schritt in die richtige Richtung. Doch lässt die

normierte Ausgestaltung der Verwendung von PIMS noch zu wünschen übrig. Die neuen Regeln des TTDSG bedeuten nicht nur, dass weiterhin auf eine Rechtsverordnung gewartet werden muss, sondern dass trotz der Verwendungsmöglichkeit weiterhin mit Cookie-Bannern gerechnet werden muss, während besonders dreiste Webseitenbetreibende die Einstellungen der PIMS-Nutzenden sanktionslos ignorieren können. Eine Nachbesserung durch den Gesetzgeber wäre an diesen Stellen wünschenswert.

In geheimer Mission

Ein forschungsspezifischer Überblick über das Geschäftsgeheimnisrecht

von Justin Rennert

Können Hochschulen und Forschungseinrichtungen Inhaber von Geschäftsgeheimnissen sein? Welche rechtlichen Schritte kann eine Hochschule oder Forschungseinrichtung unternehmen, wenn die eigenen Forschungsdaten entwendet werden und an die Öffentlichkeit gelangen? Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) ist seit etwas mehr als zwei Jahren in Kraft. Zeit für eine forschungsspezifische Betrachtung.

I. Forschung und Geschäftsgeheimnisse

Die Bedeutung von Geschäftsgeheimnissen hat in den letzten Jahren erheblich zugenommen. In der öffentlichen Diskussion war insbesondere das Thema Whistleblowing sehr präsent. Die Enthüllungen von Whistleblowern wie Julian Assange sorgten für Aufsehen und diplomatische Konflikte. Häufig folgen auf derartige Enthüllungen dann Ermittlungen der Strafverfolgungsbehörden – wegen der Verletzung von Geschäftsgeheimnissen nach dem GeschGehG.

In der Öffentlichkeit wird der Geheimnisschutz also vorrangig mit dem Whistleblowing und dessen strafrechtlichen Konsequenzen assoziiert.[1] Doch das Whistleblowing ist nur einer von vielen Fällen des Offenlegens von Geschäftsgeheimnissen. Die zivilrechtliche Seite des GeschGehG ist praktisch mindestens genauso relevant wie die strafrechtliche. Im Forschungsbereich fristet der Geheimnisschutz ohnehin vielerorts noch ein Schattendasein: Wir wollen uns dem Geheimnisschutz und dem GeschGehG in diesem Beitrag also aus der Forschungsperspektive nähern: Können Forschungsdaten Geschäftsgeheimnisse sein? Liegt sogar dann ein Geschäftsgeheimnis vor, wenn die Forschungseinrichtung gar nicht „geschäftlich" tätig ist, sondern reine Wissenschaft betreibt? Und was kann eine Forschungseinrichtung zivilrechtlich unternehmen, wenn ihre eigenen Daten unbefugterweise an die Öffentlichkeit gelangen?

Zur Beantwortung dieser Fragen schildert der Beitrag zunächst ein kurzes Beispiel (dazu unter I.). Anhand dieses Beispiels werden Voraussetzungen und Folgen des Schutzes nach dem GeschGehG erläutert (dazu unter II). Schließlich folgt eine kurze Betrachtung des Verhältnisses von Geschäftsgeheimnisschutz und Informationszugangsansprüchen (dazu III).

II. Beispielssachverhalt

Das elektrochemische Institut der Universität A forscht an der Erweiterung der Kapazität von Lithium-Ionen-Batterien. Mitarbeiter B des Instituts erhält nach Abschluss seiner Dissertation ein Angebot aus der Privatwirtschaft. Vor seinem Übertritt in das neue Unternehmen speichert er zahlreiche Unterlagen aus dem Institut auf einem USB-Stick und nimmt sie mit zu seinem neuen Arbeitgeber – obwohl er mit dem Institut eine Vertraulichkeitsvereinbarung getroffen hat. Die Unterlagen enthalten unter anderem Entwürfe einer Patentschrift für eine neue Art von Lithium-Ionen-Batterie. Diese neue Batterie hatte das Institut in den letzten Jahren entwickelt und angesichts der geplanten Anmeldung zum Patent geheim gehalten. Der neue Arbeitgeber bringt daraufhin ein eigenes Produkt auf den Markt, das auf der Forschung des Instituts und den weitergegebenen Informationen aufbaut.

1 Rennert: „Meinungsfreiheit verpflichtet", DFN-Infobrief-Recht 09/21.

III. Voraussetzungen und Folgen des Schutzes von Geschäftsgeheimnissen

Der obige Beispielssachverhalt zeigt die Relevanz des GeschGehG im Forschungskontext. Das Institut hat zwar eine Erfindung getätigt, auf diese jedoch noch kein Patent erhalten. Die Anmeldung zum Patent war bisher nur intern geplant. Sobald der neue Arbeitgeber des Mitarbeiters B die Batterie in den eigenen Produkten einsetzt und diese in Verkehr bringt, werden die Mitarbeiter des Instituts auf die Batterie kein Patent mehr erhalten. Denn das Patentrecht verlangt die Neuheit der Erfindung. Neuheit ist nur gegeben, wenn die Erfindung der Öffentlichkeit noch nicht preisgegeben wurde. Aufgrund des Patentrechts kann das Institut also eher nicht gegen B und seinen neuen Arbeitgeber vorgehen.

Möglicherweise stellten die mitgenommenen Unterlagen aber ein Geschäftsgeheimnis dar. Dann könnten das Institut und seine Mitarbeiter Schadensersatzansprüche aus dem GeschGehG gegen den Mitarbeiter B und sein neues Unternehmen haben.

1. Was ist überhaupt ein Geschäftsgeheimnis?

Was ein Geschäftsgeheimnis ist, stellt das GeschGehG in seinem § 2 dar. Grundsätzlich kann jede Information ein Geschäftsgeheimnis sein – die Information muss allerdings bestimmte Voraussetzungen erfüllen. Diese sollen im Folgenden erläutert werden.

a) Keine rein private Information

Es darf sich bei der Information nicht um eine rein private Information handeln.[2] Kein Geschäftsgeheimnis wäre also die Information darüber, wo Mitarbeiter B seine Sonntage verbringt. Die Informationen zur Lithium-Ionen-Batterie sind keine privaten Informationen, sondern solche, die bei der Forschung des Instituts entstanden sind.

b) Geheimheit der Information

Die Information ist nur dann ein Geschäftsgeheimnis, wenn sie auch tatsächlich geheim ist. Sie ist dann nicht mehr geheim, wenn sie der (Fach-)öffentlichkeit allgemein bekannt oder ohne weiteres zugänglich ist.[3] Es ist also nicht schädlich, wenn einzelne Personen Kenntnis von der Information erlangen. Es gilt vielmehr die folgende Regel: Eine Information verliert ihre Geheimheit, wenn der Personenkreis, der von ihr Kenntnis hat, nicht mehr beherrschbar ist. Einige Beispiele, in denen die Geheimheit nicht mehr gewährleistet ist:

- Wenn die Information in allgemein zugänglichen Medien oder Fachzeitschriften veröffentlicht worden ist
- Wenn sie in einer Patentanmeldung enthalten ist und das Patentamt die Anmeldungsschrift offengelegt hat
- Wenn sie im Internet frei verfügbar ist

In unserem Beispielssachverhalt handelt es sich hingegen zunächst um eine geheime Information. Denn bevor der B das Institut verlassen hat, hatte niemand außerhalb des Instituts Kenntnis von den Unterlagen. Der Personenkreis war somit beherrschbar. Nachdem der B zu seinem neuen Arbeitgeber übergetreten ist, gestaltet sich die Situation etwas schwieriger. Ist der Personenkreis noch beherrschbar? Dies hängt davon ab, wie viele Beschäftigte des neuen Arbeitgebers Kenntnis von der Information erlangen. Betreibt auch der neue Arbeitgeber eine strikte Geheimhaltung und informiert nur wenige Angestellte, so bleibt die Information wohl zunächst geheim. Spätestens ab dem Zeitpunkt, in dem der neue Arbeitgeber aber ein Batterieprodukt auf den Markt bringt, das die entwickelte Technologie des Instituts verwendet, verliert die Information höchstwahrscheinlich ihre Geheimheit.

c) Wirtschaftlicher Wert der Information

Die Information muss einen wirtschaftlichen Wert besitzen. Diese Voraussetzung ist die im Bereich der universitären Forschung wohl missverständlichste und trägt dazu bei, dass die Sensibilität für das Geheimnisschutzrecht in der Forschungspraxis gering ist (gleiches gilt für den Begriff „Geschäftsgeheimnisses“, der suggeriert, dass ausschließlich gewerbliche Stellen erfasst sind).

Deswegen sei an dieser Stelle deutlich gemacht: Die Voraussetzung des wirtschaftlichen Wertes bedeutet nicht, dass nur

2 Hoeren in Hoeren/Münker GeschGehG (1. Auflage 2021) § 2 Rn. 7 f.

3 Hoeren in Hoeren/Münker GeschGehG § 2 Rn. 11.

gewerbliche Stellen den Schutz des Geschäftsgeheimnisrechts erlangen können. Hochschulen und Forschungseinrichtungen können Inhaber von Geschäftsgeheimnissen sein. Sie bedeutet auch nicht, dass die Information einen Handelswert haben muss.[4] Ausreichend ist vielmehr ein potentieller wirtschaftlicher Wert. Dieser ist gegeben, wenn für den jeweiligen Inhaber zumindest potentiell irgendeine Art von wirtschaftlichen oder finanziellen Interessen mit der Information verbunden sind.[5] Ausreichend wäre somit zum Beispiel die Aussicht auf die Finanzierung durch Drittmittel, weil sich ein Drittmittelgeber für die Forschung an einer Universität interessiert.

Die Rechtslage zu Forschungsdaten ist somit eindeutig: Forschungsdaten können Geschäftsgeheimnisse sein. Ausgeschlossen sind nur sog. rein wissenschaftliche Erkenntnisse, also solche Informationen, die für eine kommerzielle Verwertung nicht geeignet sind.[6] In der Begründung zu einer früheren Fassung des GeschGehG fand sich noch eine Einschränkung für Forschungsdaten. Sie sollten nur vom GeschGehG erfasst sein, wenn die Forschungseinrichtung am wirtschaftlichen Wettbewerb teilnimmt. Diese Einschränkung wurde viel kritisiert und daraufhin gestrichen. Auch die Erwägungsgründe der EU-Know-How-Richtlinie beziehen Forschungsdaten ausdrücklich mit ein: Nach Erwägungsgrund 14 sollen Informationen auch dann einen wirtschaftlichen Wert besitzen, wenn die unbefugte Nutzung das wissenschaftliche Potential des Inhabers untergraben würde.

Für unseren Beispielfall bedeutet das folgendes: Die Informationen über die Lithium-Ionen-Batterien haben einen wirtschaftlichen Wert im Sinne des GeschGehG, Potentiell ließe sich damit am Markt sehr viel Geld verdienen. Und eine unbefugte Nutzung würde jedenfalls das wissenschaftliche Potenzial des Instituts schädigen. Zudem könnten sich mögliche Drittmittelgeber abwenden, wenn die Information erst einmal allgemein zugänglich ist.

4 Keller in Keller/Schönknecht/Glinke GeschGehG (1. Auflage 2021) § 2 Rn. 46

5 Hoeren in Hoeren/Münker GeschGehG § 2 Rn. 14

6 Harte-Bavendamm in Ohly/Kalbfus GeschGehG (1. Auflage 2020) § 2 Rn. 38

d) Angemessene Geheimhaltungsmaßnahmen

Für den Schutz als Geschäftsgeheimnis reicht es nicht aus, dass die Information tatsächlich geheim ist. Der Geschäftsgeheimnisinhaber muss auch nachweisen können, dass er sich aktiv um die Geheimhaltung bemüht hat. Das GeschGehG spricht insofern von „angemessenen Geheimhaltungsmaßnahmen". Welche Geheimhaltungsmaßnahmen angemessen sind, ist je nach Einzelfall unterschiedlich zu beurteilen. Der Geheimnisinhaber muss jedenfalls Maßnahmen etablieren, die seinen finanziellen Möglichkeiten angepasst sind. Das können technische, vertragliche oder organisatorische Maßnahmen sein.[7]

Technisch kann der Geheimnisinhaber sich absichern, indem er seine IT-Infrastruktur schützt und die ausgehende und eingehende Kommunikation verschlüsselt. Vertraglich ist der Abschluss von Geheimhaltungsvereinbarungen mit internen und externen Mitarbeitern ratsam. Organisatorisch ist zu denken an Mitarbeiterschulungen oder einen datensparsamen Umgang dergestalt, dass Mitarbeiter ausschließlich Zugang zu solchen Informationen erhalten, die sie zwingend für ihre Arbeit benötigen.

Entscheidend ist auch, welchen Wert die jeweilige Information für den Inhaber hat. Je bedeutsamer die Information für den Geheimnisinhaber ist, desto mehr Maßnahmen muss er ergreifen. Für unseren Beispielsfall bedeutet das Folgendes: Der Entwurf einer Patentschrift ist für das Institut sehr bedeutsam. Die Institutsleitung muss diesen daher auch stärker schützen als andere Dokumente. Für einen geschäftsgeheimnisrechtlichen Schutz spricht es, dass das Institut offenbar mit seinen Mitarbeitern Vertraulichkeitsvereinbarungen geschlossen hat (so auch mit dem später vertragsbrüchigen Mitarbeiter B).

2. Welche Folgen drohen bei einer Geheimnisverletzung?

Das GeschGehG schützt den Geheimnisinhaber sowohl vor einer unbefugten Erlangung als auch vor einer unbefugten Offenlegung oder sonstigen Nutzung. Unbefugte dürfen sich zu der Information also keinen Zugang verschaffen. Unbefugte dürfen die Dokumente, auf denen die Information enthalten ist, auch nicht Kopieren und auf einen eigenen Datenträger

7 Hoeren in Hoeren/Münker GeschGehG § 2 Rn. 18.

überführen. Unbefugte dürfen die Information auch nicht an die andere Personen oder die Öffentlichkeit weitergeben (unbefugte Offenlegung). Verboten ist zudem jegliche wirtschaftliche Verwertung der Information (unbefugte Nutzung). Etwas anderes gilt nur dann, wenn der Geheimnisinhaber ausdrücklich erlaubt hat, dass Dritte die Information erlangen, offenlegen oder nutzen. Dann liegt wiederum keine Geheimnisverletzung vor. Denn dann handelt es sich bei dem Dritten nicht mehr um einen „Unbefugten".[8] Die Erlaubnis kann – wie auch im Urheber- oder Patentrecht – im Wege einer Lizenz erteilt werden.

Die Konsequenzen bei einer Geheimnisverletzung sind vielfältig. Neben der oben bereits erwähnten strafrechtlichen Seite drohen dem Verletzer zivilrechtliche Konsequenzen: Er haftet auf Unterlassung und ggf. auch auf Schadensersatz. Zudem hat er eigene Produkte, die auf dem Geschäftsgeheimnis aufbauen, vom Markt zu entfernen.

Für unseren Beispielsfall bedeutet das folgendes: Der Mitarbeiter B begeht eine Geheimnisverletzung. Aus seinem Arbeitsvertrag ist er zur Geheimhaltung verpflichtet. Trotzdem gibt er die Information an sein neues Unternehmen weiter. Damit verwirklicht er den Tatbestand der unbefugten Offenlegung. Auch das neue Unternehmen selbst begeht eine Geheimnisverletzung. Indem es die Informationen von Mitarbeiter B entgegennimmt, verschafft es sich unbefugt Zugang zu dem Geheimnis (unbefugte Erlangung). Indem es daraufhin ein eigenes Produkt auf den Markt bringt, das auf dem Geheimnis aufbaut, verwertet es das Geheimnis wirtschaftlich und nimmt daher eine unbefugte Nutzung vor.

Sowohl der Mitarbeiter als auch das neue Unternehmen haften somit gegenüber dem Institut. Das Unternehmen müsste sein eigenes Produkt wohl vom Markt zu nehmen, wenn das Institut Klage erhebt. Denkbar sind auch Schadensersatzansprüche: Das neue Unternehmen müsste dann beispielsweise den eigenen Gewinn an das Institut abführen.

IV. Fazit

Forschungseinrichtungen können Inhaber von Geschäftsgeheimnissen sein. Das Geschäftsgeheimnisrecht ist keinesfalls nur auf gewerblich handelnde Stellen beschränkt. Um nach dem GeschGehG geschützt zu sein, müssen Forschungseinrichtungen angemessene Geheimhaltungsmaßnahmen treffen. Die Relevanz von Verschlüsselung und Schutz der eigenen IT-Infrastruktur kann nicht überbetont werden. Ratsam ist es zudem, bei den eigenen Mitarbeitern die Sensibilität für Geschäftsgeheimnisse zu erhöhen (das gilt sowohl für das Forschungs- als auch für das Verwaltungspersonal). Das Geschäftsgeheimnisrecht ist ein junges Rechtsgebiet. Vielerorts ist es daher noch unbekannt. Zu erwarten ist aber, dass die Bedeutung von Geschäftsgeheimnissen in der Forschung in den nächsten Jahren stetig zunimmt.

8 Hoeren in Hoeren/Münker GeschGehG § 4 Rn. 90.

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