DFN
infobrief recht

8 / 2020
August 2020

Ins Wasser gefallen
Privacy Shield für Datenübermittlungen über den Atlantik in die USA ungültig

Lädst du noch oder filterst du schon?
Von einem Diskussionsentwurf zur Umsetzung des Art. 17 DSM-RL, der zu neuen Diskussionen anregt

In 90 Tagen zur Verschlüsselung – der Wettlauf des Eric S. Yuan
Zu den Änderungen von „Zoom“ nach Ablauf des 90-Tage-Plans zur Verbesserung des Datenschutzes

Ins Wasser gefallen

Privacy Shield für Datenübermittlungen über den Atlantik in die USA ungültig

von Steffen Uphues

Der Europäische Gerichtshof (EuGH) hat in seinem Urteil vom 16. Juli 2020 (Rechtssache: C 311/18) das zwischen der EU und den USA bestehende Privacy-Shield-Abkommen als ungültig eingeordnet. Fraglich ist darüber hinaus, inwiefern eine Datenübermittlung in die USA weiterhin auf Standarddatenschutzklauseln gestützt werden kann. Hochschulen und Forschungseinrichtungen müssen somit etwa bei der Verwendung von Zoom darauf achten, ob die zugrundeliegenden Klauseln den Anforderungen der Datenschutz-Grundverordnung (DSGVO) genügen.

I. Vorspiel – was sagt das geltende Recht?

Nach der DSGVO dürfen personenbezogene Daten nur in ein Drittland übermittelt werden, sofern dort ein angemessenes datenschutzrechtliches Schutzniveau besteht. Deshalb sieht Art. 45 DSGVO eine Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses vor. Nach Art. 45 Abs. 3 S. 1 DSGVO steht der EU-Kommission die Kompetenz zu, einen derartigen Beschluss zu fassen. Dies geschah in Bezug auf die USA durch das Safe-Harbor-Abkommen und später durch das Privacy-Shield-Abkommen. Beide Beschlüsse richteten sich nicht auf die USA im Allgemeinen, sondern auf diejenigen Unternehmen, die unter der Aufsicht der Federal Trade Commission oder des Departments of Transportation stehen und sich zur Einhaltung der Grundsätze der Datenverarbeitung verpflichten. Voraussetzung eines Angemessenheitsbeschlusses ist – wie der Begriff erkennen lässt –, dass das jeweilige Drittland ein angemessenes Datenschutzniveau bietet. Zur Beurteilung dieser Frage lassen sich die Anhaltspunkte aus Art. 45 Abs. 2 DSGVO heranziehen.

Sofern kein Beschluss getroffen wurde, kann eine Datenübermittlung in ein Drittland auch nach Maßgabe von Art. 46 DSGVO erfolgen. Hiernach muss der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorsehen und der betroffenen Person muss ein wirksamer Rechtsschutz möglich sein. Eine geeignete Garantie kann insbesondere in der Verwendung von Standarddatenschutzklauseln bestehen. Diese Klauseln nach Art. 46 Abs. 2 lit. c DSGVO entwickelt die EU-Kommission. Sobald die Standarddatenschutzklauseln erlassen wurden, kann eine Datenübermittlung hierauf gestützt werden.

II. Wie alles begann

Das Privacy Shield war erforderlich geworden, nachdem der EuGH das zuvor verwendete Safe-Harbor-Abkommen im Oktober 2015 für ungültig erklärt hatte. Diesem Abkommen lag ein Beschluss der EU-Kommission aus dem Jahr 2000 zugrunde. Danach sollte es möglich sein, personenbezogene Daten in Konformität zur damals geltenden EU-Datenschutzrichtlinie in die USA zu übermitteln. Der österreichische Aktivist Max Schrems legte im Jahr 2013 bei der irischen Datenschutzaufsichtsbehörde eine Beschwerde gegen die Facebook Ireland Ltd. ein. Hiermit wandte er sich gegen die Datenübermittlung des Tochterunternehmens an den in den USA ansässigen Mutterkonzern. Nachdem die irische Behörde mit Verweis auf das bestehende Safe-Harbor-Abkommen untätig geblieben war, legte Schrems eine Klage auf Bearbeitung der Beschwerde ein. Der Oberste Gerichtshof Irlands legte daraufhin die Rechtssache dem EuGH zur Entscheidung vor. Dieser urteilte, das Safe-Harbor-Abkommen sei nicht gültig und die darauf basierende Datenübermittlung demzufolge rechtswidrig. Hintergrund war, dass in den USA weitreichende Befugnisse der Geheimdienste einen Zugriff auf die übermittelten Daten

ermöglichten. So waren die US-Unternehmen, die sich an das Safe-Harbor-Abkommen gebunden hatten, auf Aufforderung der US-Geheimdienste nach US-Recht dazu verpflichtet, personenbezogene Daten herauszugeben. Gegen diese Praxis konnte in den USA auch kein Rechtsweg bestritten werden. Dies wertete der EuGH als schwerwiegenden Verstoß gegen die Grundrechte der betroffenen Personen auf Achtung des Privatlebens sowie auf einen wirksamen Rechtsschutz.[1] Der Oberste Gerichtshof Irlands hob in der Folge die Zurückweisung der Beschwerde von Schrems auf. Die irische Datenschutzaufsichtsbehörde bat Schrems daraufhin, seine Beschwerde neu zu formulieren und dabei das Safe-Harbor-Urteil zu berücksichtigen. Der Österreicher kam dem nach und forderte, die Datenübermittlung, welche die Facebook Ireland Ltd. auf Grundlage von Standarddatenschutzklausen durchführte, für ungültig zu erklären.

III. Das Privacy Shield als (ungenügender) Nachfolger

Am 12. Juli 2016 hatte die EU-Kommission den Durchführungsbeschluss 2016/1250 über die Angemessenheit des vom EU-US-Datenschutzschild (Privacy Shield) gebotenen Schutzes veröffentlicht. Das Privacy Shield sollte eine Grundlage bieten, personenbezogene Daten aus EU-Ländern in die USA zu übermitteln. Die EU-Kommission war der Ansicht, dass das Privacy Shield die Voraussetzungen, die das Datenschutzrecht der EU an Übermittlungen in Drittländer aufstellt, erfülle. Dabei handelt es sich um einen Selbstzertifizierungsmechanismus für Unternehmen aus den USA. Das Privacy Shield durfte somit in der Folge angewendet werden. Der Entscheidung der EU-Kommission ließ sich allerdings nicht der Schluss entnehmen, dass in den USA generell ein angemessenes Datenschutzniveau gegeben sei. Es sollte lediglich eine EU-datenschutzkonforme Datenübermittlung in die USA ermöglicht werden.

IV. Das Urteil des EuGH

Im Privacy-Shield-Urteil äußerte sich der EuGH nun zu der umformulierten Beschwerde von Schrems und darüber hinaus generell zur Gültigkeit des Beschlusses 2010/87 über Standardvertragsklauseln sowie zum Privacy-Shield-Beschluss 2016/1250. Während der EuGH zum Schluss kommt, dass das Privacy Shield ungültig sei, erachtet er die Verwendung von Standardschutzklausen als grundsätzlich zulässig.

1. Ungültigkeit des Privacy Shield

Das Privacy Shield enthält – wie schon zuvor das Safe-Harbor-Abkommen – die Möglichkeit, dass US-Geheimdienste auf übermittelte Daten zugreifen können. Insofern finde aus Sicht des EuGH eine zu gewichtige Berücksichtigung nationaler Sicherheitsinteressen der USA statt. In einer Abwägung mit den Bestimmungen der EU-Grundrechte-Charta zur Achtung des Privat- und Familienlebens, zum Schutz personenbezogener Daten und gerade auch zum Recht auf effektiven gerichtlichen Rechtsschutz könne das Privacy Shield keine Geltung erfahren. Entscheidend sei, dass das amerikanische Recht Überwachungsmaßnahmen vorsehe, die dem im EU-Recht bedeutenden Kriterium der Erforderlichkeit nicht gerecht würden. Der Foreign Intelligence Surveillance Act – ein Gesetz zur Spionageabwehr – erlaube es den US-Geheimdiensten, in zahlreichen Konstellationen ohne richterlichen Beschluss auf übermittelte Daten zuzugreifen. Dies könne beispielsweise mit Blick auf in einer Google Cloud gespeicherte personenbezogene Daten der Fall sein. Zwar enthalte das Privacy-Shield-Abkommen Regelungen, die den US-Behörden Vorschriften bezüglich der Verarbeitung übermittelter Daten machen. Den betroffenen Personen stehe jedoch keine Möglichkeit zu, auf die Einhaltung dieser Regelungen gerichtete Rechte geltend zu machen. Insofern sei mit Blick auf den für das Verständnis und die Anwendung der DSGVO essentiellen Verhältnismäßigkeitsgrundsatzes keine Gleichwertigkeit gegeben. Auch der im Privacy Shield vorgesehene Ombudsmechanismus[2] sei nicht geeignet, etwas an der rechtlichen Wertung zu ändern. Die Einrichtung von Ombudsstellen sollte dabei helfen, dass betroffene Personen gegen Handlungen wie den Verkauf ihrer personenbezogenen Daten vorgehen können. Der EuGH bezweifelt jedoch, dass diese Stellen über einen solchen Einfluss verfügen, dass sie die Rechte betroffener Personen auch effektiv schützen können. Auch hier fehlte wohl eine rechtliche Handhabe im amerikanischen Recht.

1 Vertiefend zum Safe-Harbor-Urteil des EuGH: Sydow, Kein sicherer Hafen für die Daten?, DFN-Infobrief Recht 12/2015.

2 Commission implementing decision (EU) 2016/1250, Rn. 116.

2. Gültigkeit der Standarddatenschutzklauseln

Während das Privacy Shield somit nicht als Grundlage für die Übermittlung personenbezogener Daten dienen kann, ist die Verwendung von Standarddatenschutzklauseln weiterhin möglich. Die Klauseln werden nach Art. 46 Abs. 2 lit. c DSGVO von der EU-Kommission erlassen. Diese stellt drei verschiedene Musterverträge bereit, bei deren Verwendung eine den Anforderungen der DSGVO genügende geeignete Garantie für die Rechte der betroffenen Personen gegeben sei. Die Verträge werden auch Standardvertragsklauseln genannt. Zwei der Verträge befassen sich mit Datenübermittlungen zwischen zwei jeweils selbstständigen Verantwortlichen. Der dritte – in der vorliegenden Konstellation relevante – Vertrag regelt die Datenübermittlung an Auftragsverarbeiter in Drittländer und ist als Beschluss 2010/87 bekannt. Zwar ist dieser Beschluss aufgrund seiner Rechtsnatur als vertragliches Konstrukt für die Behörden im Land des Datenempfängers nicht maßgeblich. Entscheidend für die Gültigkeit seien laut EuGH jedoch zwei andere Komponenten. Zum einen enthalte der Beschluss wirksame Maßnahmen, durch die ein dem EU-Recht vergleichbares Schutzniveau für die Verarbeitung personenbezogener Daten eingehalten werden könne. Zum anderen seien nach dem Beschluss Datenübermittlungen auszusetzen oder zu verbieten, wenn ein Verstoß gegen die als Grundlage dienenden Klauseln vorliegt oder die Einhaltung der Vorgaben von den Beteiligten nicht zu leisten sei. Ein Schutzmechanismus wird vom EuGH hervorgehoben: Sowohl Datenexporteur als auch Datenempfänger haben im Vorfeld der Übermittlung festzustellen, ob im jeweiligen Drittland die Voraussetzung eines angemessenen Schutzniveaus gegeben ist. Sollte der Datenempfänger zum Schluss kommen, dass die Regelungen seines Landes den Standarddatenschutzklausen nicht gerecht werden, hat er dies dem Datenexporteur anzuzeigen. Dieser muss daraufhin – wie gefordert – die Übermittlung aussetzen oder sich vollends vom Vertrag lösen.

V. Fazit für öffentliche Hochschulen und Forschungseinrichtungen

Öffentliche Hochschulen und Forschungseinrichtungen sind beispielsweise in der Nutzung von Videokonferenzdiensten betroffen. Das EuGH-Urteil ist jedoch nicht gleichbedeutend damit, dass solche Dienste in Zukunft nicht mehr genutzt werden dürfen. Es ist vielmehr zu differenzieren: Das Privacy Shield kann nicht länger als Erlaubnisgrundlage für die Datenübermittlung in die USA dienen. Allerdings kann eine solche Grundlage theoretisch durch die Verwendung von Standarddatenschutzklauseln geschaffen werden. Viele Videokonferenzdienste haben auch bisher schon solche Klauseln verwendet. Hochschulen und Forschungseinrichtungen sind bei der Verwendung von Diensten wie Zoom oder Microsoft Teams für die Datenverarbeitung verantwortlich und müssen sicherstellen, dass die Klauseln geeignete Garantien zur Wahrung der Privatsphäre bieten. Dabei darf es gerade nicht zu der Konstellation kommen, dass nationale Sicherheitsbehörden ohne die Möglichkeit eines hiergegen gerichteten Rechtswegs auf personenbezogene Daten zugreifen dürfen. Zwar besteht auch in Deutschland die Möglichkeit, dass seitens der Behörden auf Daten zugegriffen wird. Die rechtlichen Hürden sind jedoch deutlich höher. Aufgrund der weiten Befugnisse der nationalen Sicherheitsbehörden ist fraglich, ob mit Blick auf die Überwachungsbefugnisse in den USA eine wirksame Standarddatenschutzklausel erstellt werden kann. Aus Sicht der irischen Datenschutzaufsichtsbehörde muss dies in der nächsten Zeit intensiv geprüft und dann rechtssicher geklärt werden.[3] Alternativ bestehen zwei weitere Möglichkeiten, auf die Entscheidung des EuGH zu reagieren: Zum einen könnten betroffene Unternehmen darüber nachdenken, Rechenzentren in Europa einzurichten oder bereits bestehende Rechenzentren zu nutzen. Andernfalls könnte für die Datenverarbeitung auch auf die ausdrückliche Einwilligung der betroffenen Person nach Ar. 49 Abs. 1 S. 1 lit. a DSGVO zurückgegriffen werden. Die Hürden für eine solche Einwilligung sind jedoch enorm hoch. Insbesondere erfordert dies, dass die betroffene Person umfassend über die Risiken aufgeklärt wird, die sich aus der Datenübermittlung in ein – der DSGVO nicht genügendes – Drittland ergeben.

3 https://www.dataprotection.ie/en/news-media/press-releases/dpc-statement-cjeu-decision.

Lädst du noch oder filterst du schon?

Von einem Diskussionsentwurf zur Umsetzung des Art. 17 DSM-RL, der zu neuen Diskussionen anregt

von Maximilian Wellmann

Der jüngst durch das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) vorgelegte zweite Diskussionsentwurf zur Umsetzung der „Richtlinie (EU) 2019/790 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG“ (DSM RL) nimmt auch die Umsetzung des hochumstrittenen Art. 17 DSM-RL in Angriff. Der Diskurs um die sog. „Uploadfilter“ hatte sich hier früh verselbständigt und eine polemische, oftmals nicht an sachlichen Kriterien ausgerichtete Debatte kreiert. Umso erstaunlicher sind die besonnenen und wohlmeinenden Reaktionen auf den zweiten Diskussionsentwurf, der versucht den gordischen Knoten zu durchschlagen und die Interessen von Diensteanbietern, Nutzern, Kreativen und Rechtsinhabern in einen angemessenen Ausgleich miteinander zu bringen. Zentrales Regelungsinstrument ist dabei der Entwurf eines gänzlichen neuen Urheberrechts-Diensteanbieter-Gesetzes (UrhDaG), dass in diesem Beitrag vorgestellt wird.

I. Hintergrund

Schon die Zustimmung der Bundesregierung zur DSM-RL wurde an den Vorbehalt gekoppelt, auf die Umsetzung von Uploadfilter nach Möglichkeit zu verzichten. Die Ernsthaftigkeit dieses Ansinnens wurde eigens in einer – allerdings rechtlich unverbindlichen – Protokollerklärung manifestiert. In Anbetracht von mehr als 170.000 Menschen, die gegen die DSM-RL auf die Straße gingen und den geäußerten Befürchtungen, die Meinungs- und Informationsfreiheit könne mit dem Einsatz von Uploadfiltern in unverhältnismäßiger Weise beschnitten werden, konnte dies als Signal an die Kritiker verstanden werden, die ins Feld geführten Bedenken ernst zu nehmen. Mit dem Inkrafttreten der DSM-RL ist es nun in der Hand des deutschen Gesetzgebers, den wohlmeinenden Absichtserklärungen auch Taten folgen zu lassen. In Ansehung der Umsetzungsfrist zum 7.Juli 2021 veröffentlichte das BMJV bereits im Januar 2020 einen ersten Diskussionsentwurf zur Umsetzung bestimmter Teilbereiche der DSM-RL. Während dieser erste Entwurf unter anderem die Umsetzung eines Leistungsschutzrechts für Presseverleger behandelte, fokussiert sich der nun vorgelegte zweite Diskussionsentwurf auf die Umsetzung des umstrittenen Art. 17 DSM-RL.[2] Entgegen den parlamentarischen Gepflogenheiten hat sich das BMJV dabei zunächst dazu entschieden zwei Diskussionsentwürfe den Referentenentwürfen voranzustellen, um im Sinne eines integrierenden Ansatzes die verschiedenen Interessengruppen frühzeitig in die nationale Umsetzung der Richtlinie einzubeziehen. Kernstück des zweiten Diskussionsentwurfs ist der Vorschlag eines neuen UrhDaG zur Verantwortlichkeit von Upload-Plattformen. Regelungstechnisch wird dabei ein völlig neues Gesetz geschaffen, das an die Seite des bestehenden Urheberrechtsgesetzes (UrhG) tritt. Begründet wird dieser Schritt mit einer Vielzahl von abweichenden Regelungen, z. B. zum Konzept der öffentlichen Wiedergabe oder zur Enthaftung von Diensteanbietern, die eine schlüssige Integration in das dogmatische Konzept des UrhG nicht zuließen.

1 Tiessen, Anfang vom Ende?, DFN-Infobrief Recht 01/2019.

2 Ausführlich Gielen, First Rule: You Do Not Talk About Uploadfilter!, DFN-Infobrief Recht 01/2020.

II. Technisches Konzept von Uploadfiltern und Kritik

Als Uploadfilter lässt sich eine automatisierte Software beschreiben, die Daten beim Hochladen ins Internet oder vor der Veröffentlichung auf einer Plattform scannt und nach bestimmten Kriterien überprüft. Die Implementierung eines Uploadfilters setzt eine Datenbank voraus, in der unzulässige Daten gespeichert werden. Die Größe der Dateien erfordert eine Speicherung in sog. Hash-Werten, bei denen es sich um kurze Buchstaben- und Zeichenfolgen handelt, die durch eine mathematische Funktion aus dem Ausgangsmaterial erzeugt werden. Ein Algorithmus vergleicht dann den Hash-Wert des hochgeladenen Materials mit dem Hash-Wert des Ausgangsmaterials. Ergibt die Auswertung eine Übereinstimmung oder eine hohe Ähnlichkeit wird der Upload verhindert. Ein vergleichbares System setzt YouTube momentan mit seinem Content-ID System ein. Rechtsinhaber können hier eine geschützte Datei in eine Referenzdatenbank hochladen. Werden nach einem Upload durch einen Nutzer Übereinstimmung mit der Referenzdatei gefunden, so kann der Rechtsinhaber optieren, ob das hochgeladene Video gesperrt wird, Werbung zugunsten des Nutzers deaktiviert wird oder aber Werbung zugunsten des Rechtsinhabers geschaltet wird. Aufgrund der Fehleranfälligkeit der eingesetzten Algorithmen wird am Konzept der Uploadfilter allerdings starke Kritik geübt. Problematisch ist vor allem, dass nach dem aktuellen Stand der Technik keine technisch zuverlässige Lösung ersichtlich ist, die eine kontextuelle Beurteilung urheberrechtlich geschützter Gestaltungen ermöglicht. Eine gesetzlich erlaubte Nutzung, wie sie beispielsweise bei der Nutzung eines Werkes im Wege der Zitierfreiheit (§ 51 UrhG) vorliegt, kann ein Uploadfilter gerade nicht erkennen. Vielmehr wird der Abgleich der Hash-Werte zwischen der Referenzdatei und der hochgeladenen Datei zu einer Übereinstimmung führen, in dessen Folge der Upload blockiert wird, obwohl eine nach § 51 UrhG rechtmäßige Nutzung des geschützten Inhalts vorliegt.

III. Wegfall der Haftungsprivilegierung für Diensteanbieter und divergierende Interessenlagen

Im Urheberrecht stehen sich typischerweise die Interessen von Nutzern, Urhebern und Rechtsinhabern gegenüber. Ergänzt wird diese klassische Interessentrias im Bereich der Online-Inhaltedienste durch Diensteanbieter (legaldefiniert in § 2 Abs. 1 UrhDaG-E). Mit § 1 Abs. 1 UrhDaG-E wird die Annahme einer eigenständigen Handlung der öffentlichen Wiedergabe für Diensteanbieter neu in die Systematik des Urheberrechts aufgenommen. Diensteanbieter können nun unmittelbar zu Adressaten von Unterlassungs- und Schadensersatzansprüchen werden, was nach der alten Rechtslage nur möglich war, wenn der Diensteanbieter bei der Wiedergabehandlung eine „zentrale Rolle“ einnahm. Diese neue Verantwortlichkeit verwehrt es dem Diensteanbieter nunmehr auch sich auf das Hostprovider-Privileg in § 10 Telemediengesetz (TMG) zu berufen, dass statuiert das Diensteanbieter mit den hochgeladenen Informationen in keinerlei Verbindung stehen. Um die neue Verantwortlichkeit der Diensteanbieter jedoch einzugrenzen, sieht das UrhDaG eine Enthaftung vor, wenn der Diensteanbieter bestimmte Sorgfaltspflichten wahrnimmt. Das UrhDaG-E statuiert hier Pflichten des Diensteanbieters im Hinblick auf den Erwerb von vertraglichen Nutzungsrechten (§ 4 UrhDaG-E), die Sperrung unrechtmäßig hochgeladener Inhalte (§ 10 UrhDaG-E) und die Entfernung dieser hochgeladenen Werke (§ 11 UrhDaG-E).

Dennoch bedeutet die Neuregelung für Diensteanbieter einen Mehraufwand. Die alte Rechtslage mit ihrem repressiven „Notice and take down Ansatz“ wird durch einen neuen präventiven Ansatz abgelöst, der es aus Sicht der Diensteanbieter erforderlich macht, urheberrechtlich geschützte Inhalte zunächst großflächig zu filtern. Diesem präventiven Ansatz ist allerdings die Gefahr eines strukturellen „Overblockings“ inhärent, mit dem die Meinungs- bzw. Informationsfreiheit der Nutzer in unverhältnismäßiger Art und Weise beschränkt werden könnte. Für die Nutzer besteht damit die Gefahr auf urheberrechtlich geschützte Informationen nur noch verzögert oder erschwert zugreifen zu können. Umgekehrt stellt die volle Verantwortlichkeit der Diensteanbieter für Rechtsinhaber eine erhebliche Erleichterung dar, da sie nicht mehr auf die mühsame Ermittlung des Täters, also der Person, die die geschützten Inhalte hochgeladen hat, verwiesen sind, sondern Unterlassungs- und Schadensersatzansprüche direkt gegen den Diensteanbieter geltend machen können.

1. Regelungen zugunsten der Nutzer

Im Zusammenhang mit den Interessen der Nutzer ist auch unweigerlich der neue § 51a UrhG-E in den Blick zu nehmen.

Dieser sieht künftig eine gesetzliche Ausnahmebestimmung zur Nutzung von Karikaturen, Parodien und Pastiche vor. § 5 UrhDaG-E greift diese Ausnahmebestimmung auf und erlaubt es Nutzern ein Werk öffentlich wiederzugeben, sofern sie sich auf eine der in § 5 Nr. 1-3 UrhDaG-E aufgezählten gesetzlichen Schrankenbestimmungen stützen können. Diese Regelung steht dabei in direktem sachlichen Zusammenhang mit der neu eingeführten Verpflichtung der Diensteanbieter, Nutzer nach § 8 Abs. 1 Nr. 2 UrhDaG-E die Möglichkeit zu eröffnen, sich beim Upload auf eine gesetzliche oder vertraglich erlaubte Nutzung stützen zu können (sog. „Pre-flagging“). Dies ist notwendig, da Algorithmen nach aktuellem Stand der Technik nicht in der Lage sind eine erlaubte Nutzung, wie z. B. die Verwendung eines Werkes unter den Voraussetzungen der Zitierfreiheit, zu erkennen und deshalb geschützte Inhalte unabhängig von ihrem Kontext immer sperren würden. Folge wäre ein „Overblocking“ rechtmäßig hochgeladener Inhalte. Der Mechanismus sieht dementsprechend vor, dass nach einem „Pre-flagging“ durch den Nutzer, es dem Diensteanbieter gem. § 8 Abs. 2 UrhDaG-E verwehrt ist diesen Inhalt zu blockieren („Online by default“). Nur wenn es sich um einen offenkundig rechtswidrigen Upload handelt und der vom Nutzer hochgeladene Inhalt zu mehr als 90% mit einem vom Rechtsinhaber gemeldeten Werk übereinstimmt, kann der Upload nach § 12 UrhDaG-E verweigert werden. Zusätzlich abgesichert werden die Nutzerinteressen zudem durch die neu vorgesehene Bagatellschranke in § 6 Abs. 1 UrhDaG-E. Diese ermöglicht es z. B. User-Generated Content in einem gesetzlich bestimmten geringfügigen Umfang (Dateien, z. B. Fotos oder Grafiken nicht größer als 250 Kilobyte, 20 Sekunden Ton oder Video und 1.000 Zeichen Text) öffentlich wiederzugeben. Dies unterliegt allerdings der Einschränkung, dass der Nutzung kein kommerzieller Zweck zugrunde liegt.

2. Regelungen zugunsten der Diensteanbieter

Die zweite zu betrachtende Gruppe sind die Diensteanbieter, die im regulatorischen Fokus des neuen UrhDaG-E stehen. Durch ihre volle Verantwortlichkeit bei der öffentlichen Wiedergabe wird das Haftungsregime zu ihren Lasten verschoben. Um jedoch einer Uferlosigkeit der Haftung entgegenzuwirken, zählt § 3 UrhDaG-E exemplarisch Dienste auf, für die das neue UrhDaG keine Anwendung findet. So unterfallen nicht gewinnorientierte Online-Enzyklopädien, wie z. B. Wikipedia nicht dem Abwendungsbereich des UrhDaG. Eine weitere Konturierung des Anwendungsbereichs erfolgt durch die Aufnahme von Bereichsausnahmen für Startup Unternehmen in der Gründungsphase (§ 2 Abs. 2 UrhDaG-E) und Kleinst-Plattformen (§ 2 Abs. 3 UrhDaG-E). Startup Unternehmen werden damit gem. § 10 Abs. 2 UrhDaG-E von der Sperrverpflichtung des Abs. 1 UrhDaG-E freigestellt, solange die durchschnittliche Anzahl unterschiedlicher Besucher der Internetseite des Dienstes 5 Millionen nicht übersteigt. Für Kleinst-Plattformen geht das Gesetz sogar noch weiter, indem widerleglich vermutet wird, dass sie aus Verhältnismäßigkeitserwägungen generell nicht zur Sperrung verpflichtet sind. Diese Regelungstechnik hat zur Folge, dass Rechtsinhaber hier den Nachweis führen müssen, weshalb eine Sperrung im konkreten Fall doch erfolgen soll. Um zudem der Gefahr des „Overblocking“ angemessen zu begegnen, sieht § 16 S. 1 UrhDaG-E eine Haftungsprivilegierung des Diensteanbieters für den Zeitraum vor, indem ein von einem Nutzer durch das „Pre-flagging“ ausgezeichneter Inhalt im Wege des Beschwerdeverfahrens (§ 14 UrhDaG-E) auf seine Rechtmäßigkeit hin überprüft wird. Auch vor sog. „False Notification“ (fälschliche Anmeldung fremder Inhalte durch vermeintliche Rechtsinhaber) werden Diensteanbieter geschützt, indem sie Rechtsinhaber nach § 19 Abs. 1 UrhDaG-E für eine angemessene Zeit von der Möglichkeit ausschließen können, Inhalte gem. §§ 10 und 11 UrhDaG-E sperren oder entfernen zu lassen.

3. Regelungen zugunsten der Rechtsinhaber

Mit der Verantwortlichkeit der Diensteanbieter geht zudem die Verpflichtung einher, entweder Lizenzen von den Rechtsinhabern zu erwerben oder Inhalte, deren Nutzung auch gesetzlich nicht erlaubt ist, zu blockieren („take down and stay down“). Auf Seiten des Diensteanbieters § 4 Abs. 1 UrhDaG-E sind deshalb „alle Anstrengungen“ zu unternehmen, die vertraglichen Nutzungsrechte zu erwerben. Was zunächst uferlos weit klingt, statuiert nach § 4 Abs. 1 UrhDaG-E jedoch lediglich einen einseitigen Kontrahierungszwang für Diensteanbieter. Ein aktives Forschen des Diensteanbieters nach Lizenzinhabern folgt aus diesem unbestimmten Rechtsbegriff nicht, was aufgrund der großen Menge an hochgeladenem urheberrechtlich geschützten Material schlichtweg unverhältnismäßig wäre. Vielmehr ist es gesetzgeberisch intendiert, dass die Nutzungsrechte dem Diensteanbieter vom Rechtsinhaber angeboten werden müssen oder über eine Verwertungsgesellschaft verfügbar sind. Der Passus „alle Anstrengungen“ ist

somit dahingehend auszulegen, dass er nur ein aktives Zugehen auf die Verwertungsgesellschaften durch die Diensteanbieter fordert. Flankiert werden diese Bestimmungen von § 10 UrhDaG-E, der für Rechtsinhaber die Möglichkeit vorsieht, den Diensteanbieter zur Sperrung seiner Werke zu verpflichten. Die Sperrpflicht unterliegt dabei ebenfalls dem Verhältnismäßigkeitsgrundsatz, was zu der Einschränkung führt das Sperrungen nur dann vorzunehmen sind, wenn dem Diensteanbieter geeignete und wirksame Mittel zur Verfügung stehen, deren Umsetzungskosten zumutbar sind.

4. Regelungen zugunsten der Urheber

Im Interesse der Urheber sieht § 7 UrhDaG-E einen Direktvergütungsanspruch gegen den Diensteanbieter für lizenzierte Inhalte vor. Auch wenn der Urheber einem Dritten das Recht der öffentlichen Wiedergabe eingeräumt hat, ist der Diensteanbieter verpflichtet, dem Urheber für die Nutzung des Werkes eine angemessene Vergütung zu zahlen. Problematisch ist allerdings, dass dieser Anspruch nur durch Verwertungsgesellschaften geltend gemacht werden kann. Um die Lizenzierung zu erleichtern und Rechtsinhaber angemessen an der Wertschöpfung zu beteiligen, sehen die neuen §§ 51 bis 51 lit. f Verwertungsgesellschaftengesetz (VGG-E) hier jedoch die Einführung sogenannter kollektiver Lizenzen mit erweiterter Wirkung vor. Diese Form der Lizenzierungspraxis soll vor allem Massennutzungen auf Plattformen erleichtern und sieht vor, dass Verwertungsgesellschaften Nutzungen auch dann gestatten dürfen, wenn ihnen die betroffenen Rechtsinhaber die Rechte zuvor nicht eingeräumt haben. Hintergrund dieser Regelung ist dabei die angemessene Partizipation außenstehender Urheber an der auf Upload-Plattformen stattfindenden Wertschöpfung.

IV. Fazit

Eins ist sicher, das Schreckgespenst des Uploadfilters, zwischenzeitlich zum Kampfbegriff in der Debatte über die Urheberrechtsrichtlinie auserkoren, hat erheblich an Schrecken verloren. Fakt ist aber auch, dass mit dem Entwurf des UrhDaG entgegen den Bezeugungen der Protokollerklärung nicht auf Uploadfilter verzichtet wird. Dennoch verfolgt das UrhDaG-E behutsam das Ziel die rivalisierenden Interessen der unterschiedlichen beteiligten Gruppen auszugleichen, sodass auch in Zukunft jeder Beteiligte seinen (wirtschaftlichen) Interessen entsprechend ein Stück vom Kuchen der digitalen Wertschöpfung erhält. Als Erfolg für die Nutzer und die Informationsfreiheit muss in diesem Kontext insbesondere die Möglichkeit des „Pre-Flagging“ bezeichnet werden. Aber auch Diensteanbieter können zufrieden sein. Zwar sind sie nunmehr bei der öffentlichen Wiedergabe von geschützten Inhalten urheberrechtlich voll verantwortlich, über die Einhaltung bestimmter Sorgfaltspflichten könne sie jedoch eine Enthaftung erreichen. Für Hochschulen und Forschungseinrichtungen wirkt sich der Entwurf zum UrhDaG nicht unmittelbar aus. § 3 Nr. 2 UrhDaG-E schließt gerade nicht gewinnorientierte bildungsbezogene und wissenschaftliche Repositorien vom Anwendungsbereich des Gesetzes aus. Nicht vergessen werden sollte allerdings, dass es sich bei dem Diskussionsentwurf nur um den Auftakt des Gesetzgebungsverfahrens handelt. Es bleibt daher spannend abzuwarten, welche Änderungen zugunsten der einen oder anderen Interessengruppe im weiteren legislativen Verfahren noch vorgenommen werden und welche konkreten Regelungen des UrhDaG-E letztlich Eingang in den finalen Gesetzestext finden.

In 90 Tagen zur Verschlüsselung – der Wettlauf des Eric S. Yuan

Zu den Änderungen von „Zoom“ nach Ablauf des 90-Tage-Plans zur Verbesserung des Datenschutzes

von Nicolas John

Die Videokonferenzplattform „Zoom“ zählt zu den Gewinnern der Corona-Krise. Doch der Erfolg brachte auch umfangreiche Kritik an der Sicherheit der Plattform mit sich. Daher kündigte der Gründer und CEO von Zoom Video Communications Eric S. Yuan am 1. April 2020 einen 90-Tage-Plan an, um den Datenschutz und die Datensicherheit der Plattform zu verbessern. Zwischenzeitlich sind die 90 Tage vergangen und Zoom besserte mit Version 5.0 erheblich nach. Doch auch der EuGH sorgt mit seinem aktuellen Urteil für Wirbel. Sind die Nachbesserungen von Erfolg geprägt?

I. Hintergrund

Während der Corona-Krise stellen Videokonferenzplattformen eines der wichtigsten Mittel zur Kommunikation dar. Besonders im Hochschul- und Forschungsbereich dienen diese der Durchführung der digitalen Lehre. Aufgrund der einfachen Bedienung und den hohen Kapazitätsgrenzen fiel in der Vergangenheit die Wahl häufig auf den Anbieter Zoom. Doch die Nutzer der Plattformen fordern aus nachvollziehbaren Gründen auch die größtmögliche Sicherheit und Schutz für die Vertraulichkeit ihrer Daten.

Mit Zunahme der Nutzer sah sich Zoom eben aufgrund mangelnder Datensicherheit und -schutzes starker Kritik ausgesetzt. So sorgten beispielsweise „Zoom-Bombings“, mangelnde Transparenz bei der Datenverarbeitung und irreführende Werbeaussagen hinsichtlich der Verschlüsselungstechnik zu Beginn der Pandemie regelmäßig für Negativ-Schlagzeilen. Auch der Bundes-, einige Landesdatenschutzbeauftragte sowie Stimmen aus der Politik warnten pauschal vor der Verwendung von Zoom.

Aufgrund dieser Kritik rief Zoom am 1. April 2020 einen 90-Tage-Plan[1] ins Leben. Ziel war vor allem – neben der Verbesserung der Voreinstellungen und der Schaffung einer besseren Transparenz – das Erreichen einer Ende-zu-Ende-Verschlüsselung („E2E-Verschlüsselung“) in Videomeetings mit mehreren Teilnehmern. Zoom sah vor, auf allen datenschutzrechtlich relevanten Ebenen nachzubessern.

Kurz vor Ablauf der 90 Tage lobte auch der baden-württembergische Datenschutzbeauftragte, entgegen seines vorherigen Kurses, die Bemühungen von Zoom.[2] Der Beitrag soll daher im Folgenden die wesentlichen Änderungen und Updates von Zoom in Augenschein nehmen und abschließend im Vergleich mit anderen Plattformen und im Kontext des jüngst ergangenen Urteils des EuGH[3] (Urteil vom 16.7.2020, Rs.: C 311/18) zum EU-US-Privacy-Shield Bilanz ziehen.

1 Abrufbar unter: https://blog.zoom.us/de/eine-nachricht-an-unsere-benutzer/ (zuletzt abgerufen am 22.7.2020).
2 Abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/warnung-des-lfdi-wurde-gehoert-zoom-bessert-nach/ (zuletzt abgerufen am 22.7.2020).
3 Vertiefend hierzu: Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 8/2020.

II. Änderungen und Updates: Ein Überblick

1. Datenschutzfreundliche Voreinstellungen

Nach den sog. „Zoom-Bombings“, bei welchen fremde Teilnehmer in Besitz des Meeting-Links ohne direkte Einladung ein Meeting stören konnten, sorgte Zoom dafür, dass standardmäßig ein zufälliges Zugangspasswort eingerichtet wird. Ebenfalls wurde ein Warteraum eingerichtet, welcher den freien Zugang zu einem Meeting mit Zugangsdaten weiter beschränken kann.
Daneben entfernte Zoom den umstrittenen „Aufmerksamkeits-Tracker“, mit welchem der Host sehen konnte, wenn ein Teilnehmer eines Meetings die App nicht im Vordergrund geöffnet hatte.

Die Facebook-Funktion wurde aus der iOS-App entfernt und neu konfiguriert, nachdem zuvor ohne Einwilligung des Nutzers Daten mit Facebook ausgetauscht wurden. Nicht erforderliche Daten werden nun nicht mehr mit Facebook geteilt. Ebenso wurde die Software für das Mac-Betriebssystem überarbeitet, um auch hier die automatische Installation eines lokalen Webservers zu unterbinden.

2. Verschlüsselung

Nachdem Zoom die Begrifflichkeit „Ende-zu-Ende-Verschlüsselung“ verwendet hatte, um lediglich die Transportverschlüsselung zu bewerben, reagierte das Unternehmen auf die Kritik zunächst mit einer Klarstellung.[4] Der Unterschied zwischen der E2E-Verschlüsselung zur Transportverschlüsselung liegt darin, dass bei der Transportverschlüsselung die Inhaltsdaten lediglich während des Übertragungsvorganges verschlüsselt werden, aber auf den Servern von Zoom wieder entschlüsselt werden und Zoom darauf zugreifen kann. Durch den Einsatz von E2E-Verschlüsselung können nur noch die Teilnehmer eines Meetings auf die Inhaltsdaten zugreifen. Serverseitige Zugriffe und Entschlüsselung - wie bei der Transportverschlüsselung - sind dagegen nicht möglich. Bei einer vollumfänglichen E2E-Verschlüsselung werden die Inhaltsdaten der Teilnehmer damit vollständig vor dem Zugriff Dritter geschützt.

Nach einem Update der Transportverschlüsselung übernahm Zoom die Firma Keybase, um mit dem Know-How eine echte E2E-Verschlüsselung zu entwickeln. Diese wird seit Juli in der Beta-Variante getestet und soll sowohl für kostenlose als auch kostenpflichtige Konten zur Verfügung stehen. Vor der Nutzung der E2E-Verschlüsselung wird es für Nutzer von kostenlosen Konten erforderlich sein, eine einmalige Authentifizierung über die Telefonnummer durchführen zu müssen. Dies soll dem eventuellen (Massen-) Missbrauch der Software für illegale Aktivitäten vorbeugen. Nicht bekannt ist bislang, wie diese Informationen von Zoom gespeichert werden. Um ein besseres und sichereres Code-Design zu erhalten, veröffentlichte Zoom im Vorfeld den Programm-Code für die E2E-Verschlüsselung.

Die E2E-Verschlüsselung wird vom Host ein- und ausschaltbar sein. Bei eingeschalteter E2E-Verschlüsselung sind einige Funktionen aus technischen Gründen nicht nutzbar. So wird es beispielsweise nicht möglich sein, sich über klassische Telefonverbindungen oder mit Konferenzraumsystemen mit SIP/H.323-Hardware in das verschlüsselte Meeting einzuwählen. Die Aktivierung bzw. Deaktivierung der E2E-Verschlüsselung wird vom Administrator auf der Konto- und Gruppenebene möglich sein.
Neben der E2E-Verschlüsselung wird die schon implementierte Transportverschlüsselung weiterhin standardmäßig verwendet werden.

3. Transparenz der Datenverarbeitung

Während des 90-Tage-Plans passte Zoom im Übrigen auch seine Datenschutzrichtlinie mehrfach an, um den Nutzern möglichst transparent zu erklären, was mit den Daten der Nutzer geschieht und wo sie verarbeitet werden. In diesem Rahmen stellte Zoom auch klar, dass die Daten nicht verkauft wurden, noch verkauft werden sollen.

4. Offene Probleme

Unabhängig von der Problematik um die Unwirksamkeit des Privacy-Shields (s. u.) muss dennoch weiterhin kritisch auf die Software von Zoom geblickt werden. Denn trotz der Überarbeitungen gibt es noch immer einige beachtenswerte Problempunkte, beispielsweise im Auftragsverarbeitungsvertrag (AVV). So schließt Zoom in seinem aktuellem „Zoom Global Data Pro-

4 Abrufbar unter: https://blog.zoom.us/facts-around-zoom-encryption-for-meetings-webinars/ (zuletzt abgerufen am 22.7.2020).

cessing Addendum“ (DPA, Stand Dezember 2019) die Löschung der personenbezogenen Daten in einem weiteren Umfang aus, als es Art. 28 Abs. 3 lit. g DSGVO zulässt. Dieser Artikel sieht vor, dass „nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder [ge]löscht oder […] [zurückgegeben werden] und die vorhandenen Kopien [ge]löscht [werden], sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung […] besteht“.
An anderer Stelle genügt Zoom seiner Informationspflicht über neue Unterauftragsverarbeiter nicht i.S.d. Art. 28 Abs. 2 S. 2 DSGVO. Danach hat der Auftragsverarbeiter grundsätzlich den Verantwortlichen über jede Änderung in Bezug auf Unterauftragsverarbeiter zu informieren, sodass der Verantwortliche ggf. Einspruch gegen die Änderung erheben kann. Nach derzeitigem Stand informiert Zoom über die Unterauftragsverarbeiter über eine in den „Datenschutzrichtlinien“ verlinkte und in dem „Zoom Global Data Processing Addendum“ unter 5.1 DPA benannte Liste. Um über Änderungen bezüglich Unterauftragsverarbeiter in Kenntnis gesetzt zu werden, hat der Verantwortliche gem. 5.1 DPA Änderungsbenachrichtigungen von Zoom zu abonnieren, um ordnungsgemäß hierüber informiert zu werden. Dies genügt nicht den Vorschriften der DSGVO, da ein aktives Handeln seitens des Verantwortlichen erforderlich ist, um über Aktualisierungen informiert zu werden.

III. Vergleich mit anderen Plattformen

Doch trotz der vergangenen Kritik steht Zoom nicht allein mit Vorwürfen hinsichtlich der Datensicherheit und des -schutzes da. Neben Zoom gibt es eine Vielzahl an anderen kommerziellen Videokonferenztools, welche ebenfalls kritisch unter verschiedenen Gesichtspunkten bewertet werden müssen.

Beachtlich ist vor allem die viel thematisierte E2E-Verschlüsselung, welche bislang lediglich bei Cisco WebEx Meetings für Videokonferenzen mit mehr als zwei Teilnehmern angeboten wird. Diese Funktion ist bei Cisco allerdings nicht standardmäßig implementiert, sondern nur auf Anfrage verfügbar. Darüber hinaus bietet bislang kein anderer Anbieter eine E2E-Verschlüsselung an.

Doch auch Cisco WebEx Meetings ist nicht frei von juristischen Mängeln. Zu kritisieren ist beispielweise, dass es bei Abschluss der Online-Bestellung an einem standardmäßigen AVV fehlt, darüber hinaus räumt sich Cisco den Vorbehalt ein, Auftragsdaten zu eigenen Zwecken zu verarbeiten.[5] Auch bei Microsoft Teams (sowie Skype for Business) finden sich derzeit im AVV Unklarheiten und Widersprüche, unzulässige Datenexporte, sowie nicht gekennzeichnete nachträgliche Änderungen im AVV.

Auch die in der Öffentlichkeit viel gelobten Anbieter Jitsi Meet und BigBlueButton nutzen in ihrer Standardkonfiguation STUN-Server in den USA, um Verbindungen aufzubauen, auch wenn sie auf selbst gehosteten Servern betrieben werden. STUN-Server haben eine ähnliche Funktion wie DNS-Server und dienen der Erkennung von Benutzer-Geräten hinter einem Router oder einer Firewall. Zudem stellt sich bei Tools wie Jitsi oder BigBlueButton auf der technischen Seite das Problem, dass nach den eigenen Angaben der Anbieter die Tools nicht so leistungsfähig sind, wie obig benannte Software. So ermöglicht Jitsi Meet auf öffentlichen Servern Videokonferenzen mit maximal 200 Teilnehmern. BigBlueButton empfiehlt selbst, nicht mehr als 100 Personen an einem Meeting teilnehmen zu lassen.

IV. EU-US-Privacy-Shield

Im Lichte des jüngst ergangenen Urteils des EuGH[6] (Urteil vom 16.7.2020, Rs.: C 311/18) hinsichtlich der Rechtswidrigkeit des Privacy-Shields-Abkommens zwischen der EU und den USA wird man trotz der stetigen Bemühungen von Zoom kritisch bei der Auswahl und Benutzung der Software bleiben müssen. Dadurch, dass viele Anbieter wie Zoom und Microsoft ihre Datenverarbeitungszentren zu großen Teilen in den USA stehen haben, ist fraglich, ob eine zulässige Übertragung der Daten in die USA ohne Privacy-Shield derzeit noch möglich ist. Denn trotz der vom EuGH festgestellten Wirksamkeit der Standardvertragsklauseln ist fraglich, ob eine Übermittlung der personenbezogenen Daten in die Vereinigten Staaten aufgrund der Klauseln rechtmäßig ist.

Doch auch Videokonferenzprogramme wie BigBlueButton und Jitsi sind hier nicht frei von datenschutzrechtlichen Fallstri-

5 Ziff. 4.c.v. Data Protection Exhibit, Attachement B des Master Data Protection Agreement, Stand Dezember 2019.

6 Vertiefend hierzu: Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 8/2020.

cken. Durch die STUN-Server in den USA und die hierbei verarbeiteten IP-Adressen als personenbezogene Daten müssen auch bei diesen Lösungen Änderungen vorgenommen werden. Bei einer Einrichtung der Software sind europäische STUN-Server zu empfehlen.

V. Fazit und Konsequenzen für die Hochschulpraxis

Trotz zahlreicher Nachbesserung seitens Zoom bleibt aufgrund der neuen Lage nach dem Urteil des EuGH das Dilemma zwischen einerseits datenschutzfreundlicher Software und andererseits performanten, aber regelmäßig datenschutzproblematischen Videokonferenztools.
Es wird daher zunächst abzuwarten sein, wie die Anbieter mit den Datenströmen in die USA im Kontext des Urteils umgehen. Allerdings hat Zoom bereits durch die vielen Nachbesserungen gezeigt, dass das Unternehmen willens ist, Datenschutz möglichst zeitnah umzusetzen. Insoweit erscheint es zumindest nicht fernliegend, dass ggf. eine rein europäische Version der Software entwickelt werden könnte. Sofern es kommerziellen Anbieter leistungsstarker Software gelingt, eine Software-Modell zu finden, welches ohne Datentransfer in die USA auskommt, wäre dies in der aktuellen Lage neben einer echten E2E-Verschlüsselung der beste Schritt Richtung Wahrung des europäischen Datenschutzniveaus.

Auch an den Hochschulen und Forschungseinrichtungen wird daher weiterhin stets auf den Zweck der Verarbeitung abzustellen sein und anhand diesem abgewogen werden müssen, welches Tool sich aus datenschutzrechtlicher Sicht überhaupt für die Umsetzung eignet.[7] Gerade hinsichtlich der technischen Möglichkeiten werden bei einigen Lösungen schnell Grenzen erreicht sein.

7 Vertiefend John, Corona is calling, DFN-Infobrief Recht Sonderausgabe zu COVID-19 4/2020.

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