DFN
infobrief recht

4/2021
April 2021

Alles in der Schwebe
Die datenschutzrechtskonforme Nutzung von Microsoft 365

Framing – The Never Ending Story feat. EuGH
Der EuGH und die neuen Leitplanken zur Auslegung der öffentlichen Wiedergabe im Urheberrecht

Steh zu deinen Fehlern oder es kommt dir teuer zu stehen
Unterlassungs- und Schadensersatzanspruch nach datenschutzrechtlichem Verstoß

Alles in der Schwebe

Die datenschutzrechtskonforme Nutzung von Microsoft 365

von Marten Tiessen

Datentransfers in die USA sind ein Thema, das die europäischen Datenschutzbehörden und Gerichte schon seit vielen Jahren beschäftigt. Bei kaum einem Thema im Datenschutz treffen Idealismus und Wirtschaftsrealität so sehr aufeinander. Welche weitreichenden Implikationen das „Schrems II"-Urteil des Europäischen Gerichtshofs (EuGH) aus dem letzten Jahr mit sich bringt, zeigt sich auch am Beispiel von Microsofts 365, der Cloudvariante des Office-Pakets. Inwiefern sich dessen Dienste zurzeit datenschutzkonform verwenden lassen, ist äußerst umstritten. Auf das Problem machten unter anderem auch der Big-Brother-Award für die baden-württembergische Kultusministerin und eine Bewertung der Datenschutzkonferenz aufmerksam. Auch für Hochschulen und Forschungseinrichtungen stellt sich die Frage, inwiefern sie die Dienste des Office-Pakets zukünftig noch nutzen können.

I. Datenschutzrechtliche Risiken bei Microsoft Office 365

Microsoft-Dienste wie Word, Excel, PowerPoint oder Outlook sind aus den Alltag kaum wegzudenken. Auch wenn sich sicherlich darüber diskutieren lässt, ob sie das technische Nonplusultra darstellen, sind diese Dienste enorm verbreitet – auch an den Hochschulen und Forschungseinrichtungen. Angeboten werden die Dienste gebündelt im Microsoft-Office-Paket, das in verschiedenen Versionen zur Verfügung gestellt wird. Office 365 oder neuerdings Microsoft 365 unterscheidet sich von anderen Office-Paketen dadurch, dass es nicht nur ein reines Software-Paket ist, sondern zugleich eine cloudbasierte Nutzung ermöglicht. Während diese Variante für Nutzer technische Vorteile bietet, erfordert sie zugleich einen ständigen Datenaustausch mit den Microsoft-Servern, um die Inhalte zu synchronisieren.

Da hierbei auch eine Vielzahl personenbezogener Nutzerdaten verarbeitet wird, ist Microsoft 365 zunehmend in den Fokus der Datenschützer geraten. Die relevanten Daten lassen sich in drei Kategorien einteilen: Funktionsdaten, die für die Bereitstellung der Dienste erforderlich sind; Inhaltsdaten, zu denen der eigentliche Inhalt von Dokumenten, Präsentationen und Emails zählt; Diagnosedaten, wie die Nutzer-ID, die Nutzungsdauer einzelner Dienste, die Größe der bearbeitenden Datei etc.

Datenschutzrechtliche Risiken bestehen dabei nicht nur im Verhältnis zwischen Microsoft und den Endnutzern. Hochschulen und Forschungseinrichtungen abonnieren Microsoft 365, um ihren Studierenden und Mitarbeitern die Nutzung der Dienste zu ermöglichen. Bei einem Großteil der Verarbeitungsvorgänge ist daher nicht Microsoft, sondern die Hochschule Verantwortliche nach Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO). Hingegen ist Microsoft in der Konstellation vielfach nur ein Auftragsverarbeiter nach Art. 28 DSGVO. Als Verantwortliche haften Hochschulen und Forschungseinrichtungen, wenn sie bei der Übertragung von Daten an die Server von Microsoft gegen Datenschutzrecht verstoßen. Die Übertragung lässt sich technisch nicht ausschließen. Allenfalls kann die Menge der erhobenen Daten durch Privacy-Einstellungen reduziert werden.

Für die verbleibenden Verarbeitungsvorgänge stellt sich die Frage, ob sie den Anforderungen der DSGVO genügen. Hieran

bestehen momentan ernsthafte Zweifel. Immer wieder wurden im letzten Jahr Datenschutzverstöße bei der Nutzung von Microsoft 365 gerügt. Beispielsweise erhielt die baden-württembergische Kultusministerin, Susanne Eisenmann, den Big-Brother-Award, weil sie Office 365 an den Schulen des Landes einsetzen wollte. Der Award ist ein Negativpreis, der an Firmen, Organisationen und Einzelpersonen vergeben wird, die nach Ansicht der Jury auf eklatante Weise Grundsätze des Datenschutzes und die Privatsphäre anderer missachten. Die Jury kritisierte unter anderem, dass durch die Nutzung von Microsoft 365 US-Sicherheitsbehörden Zugriff auf die Daten von Schülern erlangen könnten, selbst wenn die Server in der EU stehen. Auch die Datenschutzbehörden beanstandeten den Umgang von Microsoft mit personenbezogenen Daten.

II. Bewertung der DSK

Bereits im September letzten Jahres hatte die Datenschutzkonferenz des Bundes und der Länder (DSK) mit knapper Mehrheit festgestellt, dass Office 365 zurzeit nicht datenschutzkonform verwendet werden könne. Die DSK setzt sich aus den einzelnen Datenschutzbehörden der Bundesländer sowie dem Bundesdatenschutzbeauftragten zusammen und nimmt als übergeordnete Institution Stellung zu aktuellen Fragen des Datenschutzes. Nachdem die Fragen in einzelnen Arbeitskreisen aufgearbeitet werden, fasst die Konferenz ihre Ergebnisse in Entschließungen, Beschlüssen oder Stellungnahmen zusammen. Eine Prüfung der „Online Service Terms“ und Datenschutzbestimmungen für Microsoft-Onlinedienste („Data Processing Addendum“) durch den Arbeitskreis Verwaltung ergab, dass die Bestimmungen nicht den Vorgaben zur Auftragsdatenverarbeitung aus Art. 28 Abs. 3 DSGVO entsprechen. Dieser Bewertung schloss sich die DSK an. Bemängelt wurde unter anderem, dass die Art der personenbezogenen Daten und der Verarbeitungszweck nicht konkret genug beschrieben werden. Dies gelte nicht nur für Daten, die Microsoft im Auftrag verarbeitet, sondern auch für jene, die Microsoft in eigener Verantwortung für legitime Geschäftsinteressen verarbeitet. Außerdem fehle es an einer einschlägigen Rechtsgrundlage – neben dem Auftragsverarbeitungsvertrag – für die Übertragung dieser Daten, wie z.B. beim Sammeln von Telemetrie-Diagnosedaten. Das sei vor allem bei Behörden problematisch, die als Verantwortliche Daten von Beschäftigten oder Bürgern Microsoft verfügbar machen. Hier gelte aufgrund der besonderen Grundrechtsrelevanz ein verschärfter Maßstab. Außerdem könnten sich Behörden, die in Erfüllung ihrer im öffentlichen Interesse liegenden Aufgaben handeln, wegen Art. 6 Abs. 1 Satz 2 DSGVO nicht auf ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f DSGVO berufen. Damit bliebe ihnen eine wichtige Rechtsgrundlage für die Datenverarbeitung versperrt.

Nachbesserungsbedarf bestehe laut DSK auch in Hinblick auf die Offenlegung der Daten gegenüber Dritten. Microsoft gehe in seinen Datenschutzbestimmungen zwar darauf ein, dass das Unternehmen, auch wenn dies nicht den Weisungen des Kunden entspricht, gesetzlich zur Offenlegung der Daten verpflichtet sein kann. Diese Aussage sei nach Ansicht der Datenschutzbehörden aber nicht hinreichend konkret. Vorrang sollten allenfalls die Gesetze der Mitgliedsaaten oder Unionsrecht, zu dem auch Abkommen mit Drittstaaten zählen, haben. Unklar bliebe jedoch, welche Auswirkungen der US-amerikanische CLOUD Act von 2018 habe. Hiernach müssen US-amerikanische Unternehmen den Sicherheitsbehörden Zugriff auf gespeicherte Daten einräumen, auch wenn die Daten außerhalb der USA z.B. in europäischen Rechenzentren gespeichert werden. Microsoft mache zudem keine hinreichenden Angaben zur Umsetzung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO, so dass der Verantwortliche nicht bewerten könne, ob die Maßnahmen dem Risiko angemessen sind.

Die Bewertung der DSK wurde denkbar knapp von nur 9 der 17 dazugehörigen Datenschutzbehörden mitgetragen. Daher kann kaum von einer einheitlichen Beurteilung innerhalb der DSK gesprochen werden. Kritisch äußerten sich vor allem die Landesdatenschutzbehörden aus Baden-Württemberg, Bayern, Hessen und dem Saarland, die das Ergebnis als zu undifferenziert empfanden. Dies gelte insbesondere in Anbetracht der Tatsache, dass Microsoft seine Vertragsbestimmungen in der Zeit nach der Prüfung durch den Arbeitskreis Verwaltung mehrfach überarbeitet hat. Zu einer ähnlichen Bewertung wie die DSK kam allerdings auch der EU-Datenschutzbeauftragte, der Nutzern riet, alternative Dienste mit höheren Datenschutzstandards zu verwenden.

Die Einschätzung der DSK bleibt zunächst ohne konkrete Rechtsfolgen. Die Konferenz hat zugesichert, das Gespräch mit Microsoft zu suchen, um eine datenschutzkonforme Lösung zu finden. Da sich die Kritik hauptsächlich auf unzureichende Informationen in den Vertragsbestimmungen bezieht, scheint eine Nachbesserung an dieser Stelle durchaus möglich. Es

bleibt allerdings ungewiss, wie die einzelnen Datenschutzbehörden die aktuellen Vertragsbedingungen bewerten. Auch beschränkt sich die Bewertung auf den Auftragsdatenverarbeitungsvertrag. Auf die Probleme, die sich aus dem „Schrems II"-Urteil ergeben, geht die DSK hingegen überhaupt nicht ein. Hier stellt sich jedoch das deutlich größere Problem.

III. Übertragung der Daten in die USA

1. Auswirkungen von „Schrems II"

Durch das „Schrems II"-Urteil des EuGH vom 16. Juli 2020 (C-311/18) ist dem transatlantischen Datentransfer der juristische Teppich unter den Füßen weggezogen worden. In dem Urteil hat der Gerichtshof das Privacy-Shield-Abkommen zwischen der EU und den USA für unionsrechtswidrig erklärt.[1] Das Abkommen sollte eine rechtssichere Grundlage für die Übertragung personenbezogener Daten von einem EU-Mitgliedstaat in die USA bieten. Nach dem Urteil ist ein Datentransfer zwar noch über die Verwendung von Standardvertragsklauseln (SCC) zulässig.[2] Allerdings ist eine rechtmäßige Übertragung nur möglich, sofern im Drittstaat ein angemessenes Datenschutzniveau gewährleistet wird.[3] Das bedeutet, dass gegebenenfalls über die SCC hinaus noch Maßnahmen getroffen werden müssen, um die Angemessenheit des Schutzniveaus im Empfängerland sicherzustellen. Dabei kommt es auf das konkrete Schutzniveau der übermittelten Daten an und nicht auf das allgemeine Schutzniveau des Empfängerlandes. Welche zusätzlichen Maßnahmen erforderlich sind, hängt demnach vom konkreten Übertragungsvorgang und den damit verbundenen Risiken ab. Schutzmaßnahmen können die Pseudonymisierung und Verschlüsselung der Daten oder die Wahl eines Empfängers, der vor staatlichen Zugriffen geschützt ist, umfassen. Die DSK und der Bundesbeauftragte für Datenschutz und Informationsfreiheit, Ulrich Kelber, halten die Übermittlung von personenbezogenen Daten in die USA nur für zulässig, wenn solche weiteren Schutzmaßnahmen ergriffen werden. Andere Datenschutzbehörden halten die Übertragung in die USA nur in Ausnahmefällen für zulässig und wieder andere sehen zurzeit überhaupt keine Möglichkeit einer rechtmäßigen Übertragung. So rät z.B. der Europäische Datenschutzbeauftragte ganz von Datentransfers in die USA ab.

2. Ergänzung der Standardvertragsklauseln

Als Konsequenz aus dem „Schrems-II"-Urteil hat Microsoft die bisher verwendeten Standardvertragsklauseln ergänzt. Die Ergänzungen sehen vor, dass Microsoft betroffene Personen benachrichtigt, wenn dem Unternehmen durch staatliche Anordnung auferlegt wird, Daten an Sicherheitsbehörden herauszugeben. Zusätzlich verpflichtet sich Microsoft, gegen entsprechende behördliche Anordnungen bis in die letzte Instanz gerichtlich vorzugehen. Würde es dennoch zu einem unionsrechtswidrigen Zugriff der Behörden kommen, räumt das Unternehmen den betroffenen Personen einen Anspruch auf Schadensersatz gegenüber dem Unternehmen ein. Allerdings bleibt trotz dieser Ergänzungen das Grundproblem – nämlich der unverhältnismäßige Zugriff der US-amerikanischen Sicherheitsbehörden – weiterhin bestehen. Die deutschen Datenschützer sehen daher die Ergänzungen zwar als einen Schritt in die richtige Richtung, halten sie aber noch nicht für ausreichend.

IV. Fazit und Praxishinweis

Sofern Hochschulen und Forschungseinrichtungen Microsoft 365 abonnieren, sind sie für viele Verarbeitungsprozesse datenschutzrechtlich verantwortlich. Verstöße gegen die DSGVO gehen daher zu ihren Lasten. Momentan lässt sich jedoch nicht pauschal beantworten, ob und wie die Nutzung von Office 365 datenschutzkonform möglich ist. Dabei kommt es im Einzelfall auch darauf an, welche Art der Daten und für welche Zwecke sie erhoben werden. Weiterhin ist entscheidend, auf welche Server die Daten übertragen werden, bzw. in welchem Land die Server stehen. Wenn sich die Server in den USA befinden, sollten personenbezogene Daten idealerweise nur verschlüsselt übermittelt werden. Zumindest sollten die Einstellungen durch den Abonnenten so gewählt werden, dass möglichst wenig personenbezogene Daten abgeführt werden, insbesondere, wenn es sich um Diagnosedaten handelt.

---

1 Siehe hierzu ausführlich Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 08/2020.

2 Daneben ist theoretisch auch eine Übermittlung nach Art. 49 DSGVO möglich.

3 Siehe zu den Standardvertragsklauseln Wellmann, O ihr gnadenbringenden Standarddatenschutzklauseln, DFN-Infobrief Recht 12/2020.

Microsoft scheint sich zumindest zu bemühen, seine Dienste an die Vorschriften der DSGVO anzupassen. Das Problem, das bei Datentransfers in Drittländer zutage tritt, kann das Unternehmen allerdings noch nicht lösen. Es bleibt gespannt abzuwarten, was der Dialog zwischen Microsoft und hiesigen Datenschutzbehörden ergibt. Die dringendste Frage für Nutzer bleibt, ob die Behörden, die scheinbar selbst Schwierigkeiten haben, das Office-Paket datenschutzrechtlich einzuordnen, nun gegen Nutzer vorgehen. Auch wenn dies bis zum Abschluss der laufenden Gespräche mit Microsoft unwahrscheinlich ist, sollten die Nutzer die laufenden Entwicklungen genau verfolgen.

Framing – The Never Ending Story feat. EuGH

Der EuGH und die neuen Leitplanken zur Auslegung der öffentlichen Wiedergabe im Urheberrecht

von Maximilian Wellmann

Bereits im November 2019 betitelte mein ehemaliger Kollege Armin Strobel seinen DFN-Infobrief Recht mit „Framing – The Never Ending Story?“.[1] Er sollte mit seiner Prophezeiung Recht behalten, denn Anfang März diesen Jahres war es wieder so weit. Nach den letzten drei wegweisenden Entscheidungen des Europäischen Gerichtshof (EuGH) zum Urheberrecht[2], macht sich das Gericht (EuGH, Urt. v. 9.3.2021 – C- 392/19) nun daran den Schlusspunkt in der seit Jahren im Urheberrecht umstrittenen Frage des Framing zu setzen. Hierzu nimmt sich der EuGH die Auslegung des Art. 3 Abs. 1 der Informationsgesellschafts-Richtlinie (InfoSoc-RL) vor, die auf europäischer Ebene zahlreiche Verwertungsrechte des Urheberrechts harmonisiert. Höchste Zeit also, Struktur in die rechtliche Gemengelage rund um das Framing zu bringen und die Entscheidung des EuGH mit Blick auf ihre Auswirkungen für Hochschulen und Forschungseinrichtungen darzustellen.

I. Sachverhalt

Ausgangspunkt des jüngsten Urteils des EuGH ist der Streit zwischen der Verwertungsgesellschaft Bild Kunst (VG Bild Kunst) und der Stiftung Preußischer Kulturbesitz über eine Klausel in den Lizenzverträgen der VG Bild-Kunst, die die Stiftung Preußischer Kulturbesitz als Trägerin der Deutschen Digitalen Bibliothek dazu verpflichtet technische Schutzmaßnahmen gegen das Framing Dritter vorzusehen. Bei der Deutschen Digitalen Bibliothek handelt es sich dabei um eine Online-Plattform, welche deutsche Kultur- und Wissenschaftseinrichtungen miteinander vernetzt. Die Plattform funktioniert dabei als „digitales Schaufenster“. Auf ihr werden Vorschaubilder („Thumbnails“) neben weiterführenden Informationen über die Werke angezeigt. Bei diesen Vorschaubildern handelt es sich um verkleinerte Versionen der Bilder in Originalgröße. Der Nutzer hat dabei die Möglichkeit über die Digitale Bibliothek auf die Webseiten zu gelangen, auf denen die Werke in vollem Umfang öffentlich wiedergeben werden.

Um die Vorschaubilder rechtmäßig darstellen zu können, erwirbt die Deutsche Digital Bibliothek regelmäßig über entgeltliche Lizenzverträge bestimmte Rechte an den Vorschaubildern von der VG Bild-Kunst. Diese machte den Erwerb der Lizenzen aber von dem Vorliegen einer Klausel abhängig, nach der sich die Stiftung Preußischer Kulturbesitz dazu verpflichtet, wirksame technische Maßnahmen gegen das Framing der im Portal der Deutschen Digitalen Bibliothek angezeigten Vorschaubilder durch Dritte anzuwenden.

II. Technischer Einordnung des Framing

Nähert man sich der technischen Funktion des Framing, handelt es sich bei einem „Frame“ (dt. Rahmen) um den Teilbereich

1 Zum Vorlagebeschluss, Strobel, Framing – The Never Ending Story?, DFN-Infobrief Recht 11/2019.

2 Siehe hierzu, Tiessen, Was das Gesetz nicht verbietet, verbietet der Anstand, DFN-Infobrief Recht 9/2019; vgl. Wellmann, Der BGH und sein letztes Wort zum Reformistischen Aufbruch, DFN-Infobrief Recht 6/2020.

einer Website, in dem Inhalte einer anderen Website enthalten sind. Ein paradigmatisches Beispiel stellt die Einbettung eines YouTube-Videos in eine Webseite dar. Der eingebettete Teil wird dabei als „Frame“ bezeichnet. Übergeordnet funktioniert die Framing-Technik danach als Technik, nach der eine Webseite in mehrere Rahmen unterteilt wird und in einer dieser „Frames“ mittels eines anklickbaren Internetlinks („Inline-Linking“) die Inhalte einer anderen Website dargestellt werden.[3] Ziel dieser Framing Technik ist es dabei, dass den Nutzern des Webauftritts die ursprüngliche Herkunft des eingebetteten „Frames“ verborgen bleibt.

III. Urheberrechtliche Einordnung und Funktion von Verwertungsgesellschaften

Eine urheberrechtliche Dimension gewinnt das Framing durch den Umstand, dass eine unmittelbare Nutzungshandlung des Linksetzers in denjenigen Fällen angenommen wird, in denen er fremde Werke über seine Webseite den Nutzern zur Verfügung stellt und sie sich so zu eigen macht. Allerdings ist bisher nicht obergerichtlich geklärt, ob hieraus eine Verletzung des dem Urheber ausschließlich zustehenden Rechts zur öffentlichen Wiedergabe aus Art. 3 Abs. 1 InfoSoc-RL resultiert, das im deutschen Recht nicht explizit geregelt ist, systematisch aber dem § 19a Urheberrechtsgesetz (UrhG) (Recht zur öffentlichen Zugänglichmachung) zugeordnet wird.

Verwertungsgesellschaften, wie die VG Bild-Kunst, spielen im Kontext des Framing dahingehend eine Rolle, dass sie eine Intermediationsfunktion zwischen den Urhebern und den Nutzern gewährleisten. Die originäre Aufgabe von Verwertungsgesellschaften ist es, die Verwertungsreche bestimmter Urhebergruppen (Musikkünstler, Autoren, etc.) kollektiv über Wahrnehmungsverträge zu bündeln, um dann über die ihnen gem. § 31 Abs. 3 UrhG übertragenen ausschließlichen Nutzungsrechte eine bestmögliche wirtschaftliche Verwertung der Werke und sonstigen Schutzgegenstände zu ermöglichen. Der Vorteil dieser Rechtebündelung liegt für die Nutzer in dem „one stop shop“ Prinzip, da Nutzer für die Einräumung von Nutzungsrechten nicht einzeln auf den jeweiligen Urheber zugehen müssen, sondern diese zentral bei der Verwertungsgesellschaft erwerben können. Die unterschiedlichen Verwertungsgesellschaften (VG Wort, VG Bild-Kunst, etc.) unterliegen dabei nach deutschem Recht einem Kontrahierungszwang, das heißt sie sind verpflichtet, jedermann auf Verlangen zu angemessenen Bedingungen eine Lizenz zur Nutzung der ihnen übertragenen Rechte einzuräumen. Dieser Kontrahierungszwang wird jedoch durch die deutsche Rechtsprechung ausnahmsweise dann abgelehnt, wenn die Verwertungsgesellschaft dem Verlangen auf Einräumung von Nutzungsrechten vorrangige berechtigte Interessen entgegenhalten kann. Solche berechtigten Interessen sollen nach der bisherigen Rechtsprechung des Bundesgerichtshofs (BGH) gerade dann bestehen, wenn das Framing durch einen Dritten, eine öffentliche Wiedergabe des Werkes und somit eine urheberrechtlich relevante Nutzung darstellt und das Framing unter Umgehung von technischen Schutzmaßnahmen erfolgt, die der Rechtsinhaber getroffen oder einem Lizenznehmer auferlegt hat.

IV. Rechtsansicht der Parteien

Die Auferlegung technischer Schutzmaßnahmen schlägt auch den Bogen zurück zur zugrundeliegenden Entscheidung, in der dieses Vorgehen den maßgeblichen Streitgegenstand bildete. Konkret ging es um eine Lizenzabrede der VG Bild-Kunst in der eine Klausel die Stiftung Preußischer Kulturbesitz als Trägerin der Deutschen Digitalen Bibliothek dazu zwang, wirksame technische Maßnahmen gegen das Framing Dritter anzuwenden. Danach müsse es Dritten unmöglich gemacht werden, dass auf der Webseite des Berechtigten „geframte“ Werk zu entnehmen und ihrerseits selbst als „Frame“ auf ihre Webseite einzustellen. Die Stiftung Preußischer Kulturbesitz sah die streitgegenständliche Klausel dabei schon aus urheberrechtlichen Erwägungen als unwirksam an, da es sich beim Framing schon nicht um eine rechtsverletzende öffentliche Wiedergabe vgl. § 19a UrhG handele. Wenn dies jedoch bereits nicht der Fall sei, könne sie auch über die Klausel nicht in Anspruch genommen werden, technische Schutzmaßnahmen gegen eine dann schon nicht rechtsverletzende Handlung vorzunehmen.

Vor dem Landgericht Berlin (LG Berlin) erhob sie deshalb Klage auf Feststellung einer Verpflichtung der VG Bild Kunst, die Lizenzabrede auch ohne die entsprechende Klausel zu erteilen. Der Rechtsstreit gelangte bis zum BGH, der das Verfahren einstweilen aussetzte und dem EuGH im Rahmen des Vorabentscheidungsverfahren die grundlegende Frage vorgelegt hat, ob das Framing überhaupt als öffentliche Wiedergabe im

3 Siehe hierzu auch Strobel, Links, Links, Links und immer noch nicht der rechte Weg?, DFN.-Infobrief Recht 11/2016.

Sinne von Art. 3 Abs. 1 InfoSoc-RL zu bewerten ist. Wäre dies der Fall so würde diese Einordnung es der VG Bild-Kunst erlauben, die Stiftung Preußischer Kulturbesitz zur Durchführung wirksamer technischer Maßnahmen zu verpflichten.

Das der EuGH letztlich zur Auslegung des Rechts zur öffentlichen Wiedergabe überhaupt angerufen werden kann, liegt dabei in der europäischen Überformung des Ausschließlichkeitsrechts aus Art. 3 Abs. 1 InfoSoc-RL begründet, die dem EuGH die Letztentscheidungskompetenz über die Auslegung des europäischen Rechts vermittelt.

V. Entscheidung EuGH

In seiner nun ergangenen Entscheidung stellt der EuGH fest, dass sofern der Rechtsinhaber (hier die VG Bild-Kunst) beschränkende Maßnahmen gegen Framing getroffen oder veranlasst hat, die Einbettung eines Werks in die Website eines Dritten (hier die Deutsche Digitale Bibliothek) im Wege der Framing-Technik eine Zugänglichmachung dieses Werks i.S.v. Art. 3 Abs. 1 InfoSoc-RL für ein neues Publikum darstellt. Dieses Ergebnis führt nachgelagert dazu, dass die VG Bild-Kunst die Stiftung Preußischer Kulturbesitz vertraglich wirksam dazu verpflichten kann, wirksame technische Schutzmaßnahmen gegen das Framing Dritter vorzusehen. Dies folgt dabei aus der verwertungsrechtlichen Relevanz des Framings, die der EuGH in seinem Urteil für diese Fälle festgestellt hat.

Arbeitet man den entscheidenden Kern des Urteils heraus, so ist aus dem Urteil abzuleiten, dass eine rechtsverletzende öffentliche Wiedergabe i.S.v. Art. 3 Abs. 1 InfoSoc-RL nur dann vorliegt, wenn der Zugang zu den Werken durch die VG Bild Kunst beschränkt war oder sie dazu veranlasst hat, diesen zu beschränken. Da dies vorliegend der Fall war, lag ein Eingriff in das konstitutive Recht der „Zugänglichmachung des Werkes für ein neues Publikum“ vor, da die VG Bild-Kunst in diesen Fällen der freien öffentlichen Wiedergabe ihrer Werke nicht zugestimmt hatte. Diese Einordnung folgt nicht zuletzt aus dem verwertungsrechtlichen Beteiligungsgrundsatz, nach dem es dem Rechtsinhaber ohne die Einordnung als öffentliche Wiedergabe verwehrt bleibt, eine angemessene Vergütung für die Nutzung seiner Werke zu verlangen.

Unterliegt die Werknutzung im Rahmen des Framings allerdings keinen rechtsinhaberseitigen Beschränkungen, hat dieser von Anfang an die Wiedergabe seiner Werke gegenüber sämtlichen Internetnutzern erlaubt, sodass im Ergebnis keine öffentliche Wiedergabe durch die Framing-Technik vorliegt. Insofern zeigt sich die Quintessenz des EuGH Urteils darin, dass sie den Rechtsinhabern einen differenzierenden Weg aufweist und es letztlich ihnen anheimstellt, ob sie wirksame technische Schutzmaßnahmen implementieren bzw. einem Dritten auferlegen, damit das Framing als Eingriff in das Recht auf öffentliche Wiedergabe zu beurteilen ist. In Fällen in denen die Rechtsinhaber von solchen Maßnahmen oder Vorgaben absehen, ist das Framing durch Dritte weiterhin nicht als Eingriff in das Recht auf öffentliche Wiedergabe anzuerkennen.

VI. Fazit und Ausblick

Für die streitgegenständliche Klausel der VG Bild-Kunst bedeutet das Urteil, dass sie die Stiftung Preußischer Kulturbesitz wirksam dazu verpflichten kann, wirksame technische Schutzmaßnahmen gegen das Framing der im Portal der Deutschen Digitalen Bibliothek angezeigten Vorschaubilder durch Dritte anzuwenden. Die grundsätzlich nutzerfreundliche Rechtsprechung des EuGH schlägt somit einen bisher nicht gekannten Schlenker zugunsten der Rechtsinhaber.

Für Hochschulen und Forschungseinrichtungen, ist mit dem Urteil des EuGH zu befürchten, dass sie in Zukunft durch die Verwertungsgesellschaften vertraglich verpflichtet werden können, eigene technische Schutzmaßnahmen gegen Dritte vorzusehen, damit Dritte auf der Hochschulwebseite „geframte Werk“ nicht ungehindert kopieren und auf ihrer eigenen Webseite „framen“ können. Insoweit ist durch das Urteil ein Mehraufwand zu erwarten, der die Hochschulen und Forschungseinrichtungen grundsätzlich dazu aufruft, sich Gedanken über technische Schutzmaßnahmen für Werke und sonstige Schutzgegenstände des Urheberrechts zu machen. Allzu viel Zeit sollten die Hochschulen und Forschungseinrichtungen jedoch nicht ins Land gehen lassen, ist doch zu vermuten, dass der BGH den Rechtsstreit noch 2021 abschließend entscheiden wird und die skizzierte Auslegung des EuGH zum Recht der öffentlichen Wiedergabe sich dann auch in der obergerichtlichen deutschen Rechtsprechung niederschlagen wird. Seien Sie also beruhigt, die „Never Ending Story“ des Framing wird schon bald fortgesetzt.

Steh zu deinen Fehlern oder es kommt dir teuer zu stehen

Unterlassungs- und Schadensersatzanspruch nach datenschutzrechtlichem Verstoß

von Steffen Uphues

In einem Urteil des Landesgericht (LG) Darmstadt vom 26.Mai 2020 (Az. 13 O 244/19) äußerten sich die Richter:innen zum Schadensersatzanspruch aus Art. 82 Abs. 1 Datenschutz-Grundverordnung (DSGVO): Wird eine Mail mit personenbezogenen Daten versehentlich an den falschen Empfänger versendet, könne dies einen Verstoß gegen Art. 6 Abs. 1 DSGVO darstellen und einen Unterlassungs- und Schadensersatzanspruch nach sich ziehen. Spätestens wenn darüber hinaus eine Meldepflicht nach Art. 34 DSGVO ausgelöst wird, aber unbeachtet bleibt, kann es teuer werden.

I. Sachverhalt

Im Zuge eines Bewerbungsverfahrens sendete eine Bank mit einem Bewerber Nachrichten hin und her. Eine dieser Nachrichten wurde seitens der Bank im Portal Xing versehentlich an eine unbeteiligte Person weitergeleitet. Die Nachricht umfasste verschiedene Informationen und nahm unter anderem auf die vom Bewerber geäußerte Gehaltsvorstellung Bezug. Die am Bewerbungsverfahren unbeteiligte Person war dem Bewerber aus gemeinsamen beruflichen Zeiten bekannt und informierte diesen darüber, dass die Nachricht an ihn versendet wurde. Dies teilte er auch der Bank mit. Dennoch wurde der Bewerber von der Bank nicht über den Vorgang informiert. Zunächst äußerte sich der Bewerber gegenüber der Bank nicht zu der Angelegenheit. Nachdem er jedoch aus dem Bewerbungsverfahren ausgeschieden war, wendete er sich an die Bank und fragte, wie es zum Versand der Nachricht an einen Unbeteiligten kommen konnte. Ebenso brachte er seine Verwunderung darüber zum Ausdruck, dass er von der Bank nicht darüber informiert worden war. Der externe Datenschutzbeauftragte der Bank vertrat in der Antwort den Standpunkt, dass kein datenschutzrechtlicher Verstoß vorgelegen habe.
Der Bewerber erhob daraufhin Klage gegen die Bank. Diese sollte eine Unterlassungserklärung abgeben und Schadensersatz in Höhe von 2.500 € zahlen. Ein Schaden sei ihm unter anderem dadurch entstanden, dass der unbeteiligte Dritte – der potentiell mit dem Bewerber um ausgeschriebene Stellen konkurriert – die Informationen für sich nutzen kann und einen Vorteil im Bewerbungsprozess erlangt.

II. Urteil

Generell hat das LG Darmstadt eine Verletzung der informationellen Selbstbestimmung aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG angenommen. Die relevante Nachricht enthalte personenbezogene Daten. Das Versenden an den falschen Empfänger stelle insofern einen Verstoß gegen die DSGVO dar, da keine taugliche Erlaubnisgrundlage aus Art. 6 DSGVO vorlag. Die Bank hatte im Laufe des Verfahrens angeführt, dass lediglich der Nachname des Bewerbers in der Nachricht enthalten und die Person demnach nicht zu identifizieren war. Diese Begründung teilte das LG Darmstadt nicht. In Kombination mit den anderen enthaltenen Informationen wie Geschlecht oder der Bezeichnung „Händler“ sei eine eindeutige Identifizierung des Bewerbers möglich gewesen. Insbesondere gelte dies auch für Personen, die – anders als der Empfänger im vorliegenden Fall – den Bewerber bislang nicht kannten.

Das Gericht hat in seiner Entscheidung geäußert, dass dem Bewerber ein Anspruch auf Unterlassung nach §§ 823 Abs. 1 i.V.m. 1004 Abs. 1 S. 2 BGB i.V.m. Art. 6 DSGVO zustehe. Insbesondere entfalte die DSGVO keine Sperrwirkung, sodass Unterlassungsansprüche neben dem Regelungswerk der DSGVO

bestehen können. Die Bank muss es demnach unterlassen, in der Zukunft auf die bisherige – fehleranfällige – Art und Weise personenbezogene Daten des Bewerbers zu verarbeiten. Hiergegen versuchte sich die Bank zur Wehr zu setzen, indem sie anführte, es bestehe keine Wiederholungsgefahr. Das Vorliegen einer solchen Gefahr ist eine Voraussetzung für das Vorliegen eines Unterlassungsanspruchs. Bei einem bereits erfolgten Verstoß geht man in der rechtlichen Bewertung zunächst von einer Wiederholungsgefahr aus. Diese Vermutung lässt sich zwar widerlegen – jedoch gelang dies der Bank im vorliegenden Fall nicht. Es konnte im Nachgang zum Verstoß keine umfassende Aufklärung und Schulung der zuständigen Mitarbeiter:innen der Bank nachgewiesen werden. Solche Maßnahmen sind abstrakt betrachtet dazu in der Lage, eine mögliche Wiederholungsgefahr „aus der Welt zu schaffen". Die Aussagen des im Verfahren gehörten Zeugen ließen aber nicht darauf schließen, dass alle Mitarbeiter:innen strukturiert auf das strikte Einhalten der Vorgaben aus Datenschutzrecht und Datensicherheit trainiert wurden. Der Unterlassungsanspruch ist auch nicht dadurch ausgeschlossen, dass der Bewerber den Verstoß erst nach Ausscheiden aus dem Bewerbungsverfahren angemerkt hat. Aus dem weitergeführten Prozess könne nicht der Rückschluss gezogen werden, er nehme den Datenschutzverstoß ohne weiteres hin. Das Gericht wies auch darauf hin, dass für den Bewerber die Gefahr bestand, im Bewerbungsverfahren nicht mehr berücksichtigt zu werden, sobald er auf den Vorgang aufmerksam gemacht hätte.

Aufgrund des Vorgangs steht dem Bewerber nach Ansicht des LG Darmstadt ebenso ein Anspruch auf Schadensersatz aus Art. 82 Abs. 1 DSGVO zu. Der hierfür erforderliche Verstoß gegen die DSGVO ergebe sich aus der fehlenden Erlaubnisgrundlage für die Weiterleitung (Art. 6 Abs. 1 lit. a DSGVO) sowie aus dem Umstand, dass der Bewerber als betroffene Person nicht unverzüglich über das daraus resultierende Risiko informiert wurde (Art. 34 DSGVO). Die Meldepflicht nach Art. 34 DSGVO setzt voraus, dass voraussichtlich ein hohes Risiko für die betroffene Person entsteht. Aus Sicht des Gerichts war dies vorliegend der Fall. Der Schaden sei durch das Weiterleiten der Nachricht bereits eingetreten, denn der Bewerber hatte keine Kontrolle mehr darüber, wer im Besitz der Informationen war. Es war etwa nicht auszuschließen, dass der jetzige Arbeitgeber des Bewerbers von dem Bewerbungsverfahren Kenntnis erlangt.
Den immateriellen Schaden, der mit dem Anspruch aus Art. 82 Abs. 1 DSGVO geltend gemacht werden kann, sah das Gericht darin begründet, dass die in der Nachricht enthaltenen Informationen zumindest abstrakt dazu geeignet seien, der weiteren beruflichen Entwicklung des Bewerbers zu schaden. Da jedoch lediglich ein einziger unbeteiligter Dritter unbeabsichtigter Empfänger der Nachricht war, empfand das Gericht die Forderung nach 2.500 € als zu hoch und setzte eine Schadensersatzforderung in Höhe von 1.000 € an.

III. Fazit und Konsequenzen für die Praxis in wissenschaftlichen Einrichtungen

Das LG Darmstadt macht in seinem Urteil deutlich, dass es sich bei derartigen Verstößen nicht um „Kavaliersdelikte" handelt. Hieraus sind zwei Lehren zu ziehen. Zunächst sollten Hochschulen und Forschungseinrichtungen ein gutes Konzept zur Sensibilisierung und Schulung ihrer Mitarbeiter:innen entwerfen und anwenden. Im besten Fall lassen sich durch verantwortungsbewusstes Handeln schon viele Verstöße vermeiden. Zumindest kann ein überzeugendes Konzept helfen, Argumente gegen das Vorliegen einer Wiederholungsgefahr zu sammeln.

Darüber hinaus ist mit Blick auf das Entstehen immaterieller Schadensersatzansprüche davon auszugehen, dass insbesondere ein Verstoß gegen die Meldepflicht aus Art. 34 DSGVO schwer ins Gewicht fällt. Frei nach dem Motto: Das Geringste, was du tun kannst, ist, zu deinen Fehlern zu stehen und die Leidtragenden zu informieren. Insofern sollten Hochschulen und Forschungseinrichtungen Hinweisen auf möglicherweise rechtswidrige Datenverarbeitungen nachgehen und diejenigen, für deren persönliche Freiheit sich hieraus ein hohes Risiko ergeben kann, schleunigst in Kenntnis setzen.

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