NEU: Podcast der
Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

7 / 2022
Juli 2022

Nicht verzagen, sondern klagen

Der EuGH zur Klagebefugnis von Verbraucherverbänden bei Datenschutzverstößen

von Klaus Palenberg

Der Gerichtshof der Europäischen Union (EuGH, Urteil vom 28.04.2022 - C-319/20) hat entschieden, dass Verbraucherschutzverbände auch nach Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) bei Datenschutzverstößen die Rechte der Verbrauchenden gerichtlich geltend machen dürfen. Damit räumt er die vom Bundesgerichtshof (BGH) in seinem Vorlagebeschluss geäußerten Zweifel aus dem Weg, die DSGVO verbiete eine unabhängige Geltendmachung von Datenschutzverstößen ohne Auftrag Betroffener. Dies stärkt die Rechtsdurchsetzung im Bereich des Datenschutzes in Deutschland, welche bislang ohne Rechtsunsicherheiten insbesondere auf die Aufsichtsbehörden beschränkt war.

I. Der Hintergrund des Verfahrens

Das der EuGH-Entscheidung zu Grunde liegende Verfahren hat schon eine längere Geschichte hinter sich. Bereits im Jahre 2014 strengte der Verbraucherzentrale Bundesverband (vzbv) ein Verfahren gegen Facebook an, in dem er Verstöße von Facebooks „App-Zentrum“ gegen das Datenschutzrecht, das Recht zur Bekämpfung unlauteren Wettbewerbs und das Verbraucherschutzrecht rügte. In seinem App-Zentrum bot Facebook seinen Benutzern verschiedene Apps an. Darunter waren auch kostenlose Online-Spiele, wie z.B. der Klassiker Scrabble. Der vzbv bemängelte unter anderem, dass die für die Verarbeitung von personenbezogenen Daten erforderliche Einwilligung von Facebook nicht in korrekter Weise eingeholt worden ist. Der zur Teilnahme an den Spielen notwendige Klick auf den Button „Sofort spielen“ war nach seiner Ansicht nicht dazu geeignet, die mit der Spielteilnahme einhergehende Übertragung personenbezogener Daten zu rechtfertigen. Unter dem Button erschien folgende Information:
„Durch das Anklicken von „Spiel spielen“ oben, erhält diese Anwendung:
- Deine allgemeinen Informationen (?)
- Deine E-Mail-Adresse
- Über dich
- Deine Statusmeldungen

Diese Anwendung darf in deinem Namen posten, einschließlich dein Punktestand und mehr.“

Diese Informationen waren jedoch nach Ansicht des vzbv nicht dazu geeignet, die Verbrauchenden in die Lage zu versetzen, eine bewusste und freiwillige Entscheidung über die Preisgabe ihrer Daten zu treffen. Darin sah er sowohl Verstöße gegen das Wettbewerbsrecht als auch das Bundesdatenschutzgesetz und das Telemediengesetz, sowie die Verwendung unwirksamer Allgemeiner Geschäftsbedingungen.

Mit dieser Argumentation hatte der vzbv dann sowohl vor dem Landgericht Berlin als auch dem Kammergericht Erfolg. Nachdem Facebook Revision eingelegt hatte, gelangte das Verfahren schließlich zum BGH. In Hinblick auf die Datenschutzverstöße stimmte dieser den Vorinstanzen zu und hielt die Klage des vzbv für begründet. Auch seiner Auffassung nach verstieß das App-Zentrum von Facebook in seiner damaligen Form gegen geltendes Recht.

Allerdings hatte der BGH Zweifel daran, ob der vzbv überhaupt befugt war, die Klage zu erheben. Denn in der Zwischenzeit war am 25. Mai 2018 die DSGVO in Kraft getreten. Diese ändere, so der BGH, zwar nichts an der Begründetheit der Klage, doch sei fraglich, ob der vzbv noch klagebefugt sei.
Zur Erklärung ist darauf hinzuweisen, dass die Klagebefugnis im Rahmen der Zulässigkeit der Klage geprüft wird. Nach

deutschem Zivilprozessrecht muss die Zulässigkeit einer Klage nicht nur zu Beginn des Verfahrens vorliegen, sondern über alle Instanzen hinweg, und in jeder Instanz wird erneut geprüft, ob sie weiterhin besteht.

II. Die Vorlagefrage

Der vzbv hatte sich zur Begründung seiner Klagebefugnis auf Normen des Gesetzes gegen den unlauteren Wettbewerb (§ 8 Abs. 3 UWG) und des Unterlassungsklagegesetzes (§ 3 Abs. 1 Satz 1 Nr. 1 UKlaG) gestützt. Insbesondere mit diesen Regelungen hatte der deutsche Gesetzgeber eine Verbandsklagebefugnis geschaffen. Damit sind u.a. sogenannte „qualifizierte Einrichtungen", die sich in öffentliche Verzeichnisse haben eintragen lassen, berechtigt, Wettbewerbsverstöße und Verbraucherschutzverstöße selbst geltend zu machen. Ohne entsprechende Regelungen stünden diese Ansprüche jeweils nur den unmittelbar Betroffenen selbst zu, so dass lediglich Mitbewerber bzw. Verbrauchende klagen dürften. Als qualifizierte Einrichtung i.d.S. durfte der vzbv also auch die hier im Raum stehenden Unterlassungsansprüche wegen Wettbewerbs- und Datenschutzverstößen nach diesen Regelungen in eigenem Namen geltend machen.
Zum Zeitpunkt der Klageerhebung im Jahr 2014 bestand die Klagebefugnis des vzbv als Verbraucherschutzverband daher auch ohne große Zweifel. Hierin waren und sind sich alle Gerichte, auch der BGH, einig. Mit Inkrafttreten der DSGVO im Jahr 2018 konnte sich aber die Rechtslage geändert haben. Die DSGVO gilt seit 2018 in allen Mitgliedsstaaten und damit auch in Deutschland unmittelbar. Damit ist nationales Recht, das nicht mit der Verordnung vereinbar ist, nicht anwendbar. Dies konnte nach Ansicht des BGH auch für besagte Normen des UWG und des UKlaG gelten. Denn, so argumentierte der BGH, könnte die DSGVO eine abschließende Regelung bezüglich der Vertretung von betroffenen Personen enthalten. Dies hätte zur Folge gehabt, dass die nationalen Regelungen, auf die sich der vzbv zur Begründung seiner Klagebefugnis gestützt hatte, unanwendbar gewesen wären. Der vzbv hätte sich bezüglich seiner Rüge von Verstößen gegen das Datenschutzrecht dann nur noch direkt auf die DSGVO berufen können.

Hierin sah der BGH aber ein Problem: Art. 80 Abs. 1 der DSGVO erlaube ein Tätigwerden von Organisationen nämlich nur im Auftrag einer betroffenen Person. Ein solcher Auftrag lag hier aber gerade nicht vor. Der vzbv war auf eigene Initiative hin, also ohne dahinterstehende einzelne Verbrauchende, tätig geworden. Auch Art. 80 Abs. 2 DSGVO helfe nicht, denn hiernach sei eine tatsächliche Verletzung von Rechten konkret betroffener Personen erforderlich. Ebenso sah der BGH keine Verbandsklagebefugnis in Art. 84 Abs.1 DSGVO, wie sie nach § 8 Abs. 3 UWG vorgesehen ist.

III. Die Entscheidung

Diese Bedenken teilt der EuGH jedoch nicht und sieht die Klagebefugnis des vzbv als gegeben an.
Zunächst bestätigt er den BGH darin, dass die DSGVO eine grundsätzlich vollständige Harmonisierung der Rechtsvorschriften zum Schutz personenbezogener Daten bezwecke. Allerdings sieht der EuGH die Lösung des Problems, im Gegensatz zum BGH, im zweiten Absatz des Art. 80 DSGVO. Dieser lasse nämlich den Mitgliedstaaten einen Spielraum dahingehend, Regelungen vorzusehen, nach denen Organisationen auch ohne einen Auftrag durch eine betroffene Person tätig werden können. Die Regelungen des UWG und des UKlaG, auf die sich der vzbv gestützt hatte, füllen diesen Spielraum auch aus. Insoweit betreffe der Anwendungsvorrang der DSGVO diese Normen deshalb nicht. Somit könne sich der vzbv zur Begründung ihrer Klagebefugnis auch auf diese stützen.

Dass der vzbv ohne Auftrag tätig geworden ist, sei vor diesem Hintergrund unschädlich. Zudem sei auch nicht erforderlich, dass der vzbz vorweisen könne, dass es bei einer bestimmten Person tatsächlich zu einer Rechtsverletzung gekommen ist. Es reiche aus, dass nach der Einschätzung des vzbv die Datenverarbeitung die Rechte identifizierbarer natürlicher Personen betreffen könne, ohne dass ein bei einer bestimmten Person eingetretener Schaden nachgewiesen werden müsse. Voraussetzung sei nur, dass der vzbv den sonstigen Voraussetzungen des Art. 80 Abs. 1 DSGVO entspreche, dass er also insbesondere ein Ziel verfolge, das im öffentlichen Interesse läge und er zum Schutz der Rechte und Freiheiten von betroffenen Personen tätig werde. Das sei für einen Verbraucherverband wie dem vzbv aber problemlos zu bejahen. Damit stand der Klagebefugnis des vzbv in den Augen des EuGH nichts mehr im Weg.

IV. Folgen für die Hochschulen

Die Entscheidung hat für wissenschaftliche Einrichtungen in zweierlei Hinsicht große Bedeutung. Zum einen besteht für private Institutionen weiterhin die Gefahr, Ziel einer Abmahnung durch

Verbraucherverbände zu werden. Dies betrifft zum Beispiel Fälle, in denen private Forschungseinrichtungen personenbezogene Daten von Verbrauchenden erhoben haben und diese verarbeiten möchten. Hier können die Verbraucherschutzverbände die Einhaltung der datenschutzrechtlichen Vorgaben auch ohne einen Auftrag eines Verbrauchenden abmahnen und schließlich auch gerichtlich durchsetzen.

Zum anderen ist damit zu rechnen, dass nach Klärung der verfahrensrechtlichen Unwägbarkeiten auch inhaltliche Entscheidungen zum Datenschutzrecht getroffen werden. Nach dem nun klar ist, dass Verbraucherverbände klagebefugt sind, werden eine Reihe von bereits laufender und neuer Verfahren entschieden werden können. Dabei werden dann hoffentlich eine Vielzahl der auch vier Jahre nach Inkrafttreten weiterhin offenen Fragen in Bezug auf die Auslegung der DSGVO beantwortet werden. Dies hätte eine enorm gesteigerte Rechtssicherheit für alle Beteiligten, zu denen sämtliche Hochschulen zählen, zur Folge.

Mein, Dein, das sind doch nicht nur bürgerliche Kategorien!

Zu den rechtlichen Hürden beim Einsatz von Plagiatsüberprüfungssoftware

von Owen Mc Grath

Zur Kontrolle von aufwendigen Prüfungsarbeiten auf Plagiate bietet sich gerade an Hochschulen der Einsatz von Plagiatssoftware an. Auch eine Archivierung von bereits überprüften Arbeiten scheint in diesem Zusammenhang sinnvoll. Das Urheber- und Datenschutzrecht ist hierbei aber nicht aus den Augen zu verlieren.

I. Einsatz von Software

Hochschulen sind durch die Hochschulgesetze aufgefordert, Prüfungsarbeiten, welche bei ihnen abgelegt werden, zu überprüfen. Dies hat nach den „Grundsätzen guter wissenschaftlicher Lehre“[1] zu geschehen. Zu diesen Grundsätzen gehört auch, die Arbeit auf Plagiate zu überprüfen. Hierzu werden bereits vielerorts Computerprogramme eingesetzt. Bevor die rechtlichen Hürden beleuchtet werden können, ist ein kurzer Blick auf die Funktionsweise solcher Software zur Plagiatskontrolle zu werfen.

II. Funktionsweise

Die grundlegende Funktionsweise von Plagiatssoftware lässt sich schnell umreißen. Ein zu überprüfender Text wird in ein Programm eingelesen und daraufhin mit vorher festgelegten und zur Verfügung stehenden Texten abgeglichen. Ergeben sich nicht gekennzeichnete Überschneidungen zwischen Prüftext und Referenztexten, meldet die Software diese Überschneidungen. Auch Strukturplagiate, die nicht den gleichen Wortlaut verwenden, aber einen gleichen Aufbau haben (bspw. gleiche Überschriften), können so aufgedeckt werden. Meldet die Software einen Plagiatsverdacht, muss in aller Regel noch eine händische Überprüfung und Bestätigung erfolgen.

An Hochschulen kann eine solche Software auf eigenen Servern, aber auch extern auf den Servern eines dritten Anbieters betrieben werden.
Die Effizienz einer Software ist im Rahmen der Plagiatsüberprüfung unbestritten. Selbst wenn sich die Kontrolle auf größere Arbeiten wie Doktor- oder Abschlussarbeiten beschränken würde, wäre ein Mensch niemals in der Lage, eine solche Vielzahl von Texten mit auch nur ansatzweise so vielen Quellen zu vergleichen.

III. Urheberrechtliche Probleme

Prüfungsarbeiten können je nach Ausgestaltung ein urheberrechtliches Werk darstellen. Voraussetzung hierfür ist nach § 2 Abs. 2 Urheberrechtsgesetz (UrhG) insbesondere das Erreichen einer gewissen Schöpfungshöhe. Simple Klausuren zum Ankreuzen oder mathematische Aufgaben, deren Lösungsweg der Sache nach schon vorgegeben ist, erreichen diese Höhe nicht. Umfangreichere Essays, Bachelor-, Master oder Doktorarbeiten sind jedoch in aller Regel als urheberrechtliche Werke einzuordnen.
Das Urheberrechtsgesetz sieht bestimmte Ausschließlichkeitsrechte des Urhebers vor (§ 15 UrhG), welche grundsätzlich nur diesem zustehen. Unter diese fällt auch das Recht der Vervielfältigung. Bei der Plagiatskontrolle via Software ist eine solche Vervielfältigung (bspw. Laden in den Arbeitsspeicher) technisch notwendig.

1 So bspw. in: § 58 Abs.2 Hochschulgesetz NRW

Um Handlungen, welche die Ausschließlichkeitsrechte des Urhebers betreffen, rechtmäßig durchführen zu können, bestehen mehrere Möglichkeiten. Zum einen besteht die Möglichkeit, das Handeln durch eine sogenannte Schranke des Urheberrechts zu rechtfertigen. Bei diesen Schranken handelt es sich um gesetzliche Vorschriften des UrhG, die ein Handeln unter bestimmten Voraussetzungen zulassen, ohne dass hierfür die Zustimmung des Urhebers notwendig wäre. Die zweite Option besteht darin, sich die Erlaubnis zur Verwendung des Werkes einzuholen. Das kann durch eine schlichte Zustimmung oder durch eine vertragliche Einräumung von Nutzungsrechten geschehen.

Als Schranken für den Einsatz von Plagiatssoftware an Hochschulen kommen der § 44a UrhG, welcher vorrübergehende Vervielfältigungshandlungen genehmigt, und der § 60d UrhG, welcher Text und Data Mining im wissenschaftlichen Kontext erlaubt, in Frage. Bei beiden Schranken tun sich jedoch Probleme auf.
Der § 44a UrhG hat einen sehr engen Anwendungsbereich und erlaubt nur solche Vervielfältigungen, die z.B. technisch notwendig sind und nur vorübergehender Art sind. Werden Prüfungsarbeiten mithilfe einer Software auf Plagiate überprüft, ist es notwendig, dass diese Arbeiten in das Programm eingelesen werden. Hierbei handelt es sich nicht um eine bloß vorübergehende Vervielfältigungshandlung im Sinne des § 44a UrhG. Mithin ist nicht jede Vervielfältigungshandlung im Rahmen der Plagiatsüberprüfung über diese Schranke zu rechtfertigen.

Der § 60d UrhG erlaubt Vervielfältigungen von Werken für Text und Data Mining zum Zwecke wissenschaftlicher Forschung. Text und Data Mining kann definiert werden als massenhafte durch einen Algorithmus gesteuerte Verarbeitung von Daten und Texten zur Erkennung von Bedeutungsstrukturen. Auch eine Plagiatssoftware verarbeitet gesteuert durch einen Algorithmus massenhaft Texte zur Erkennung von Übereinstimmungen. Die grundlegende Tätigkeit kann also dem § 60d UrhG zugeordnet werden. Problematisch ist nur, dass die Norm die Vervielfältigung nur zu Zwecken der wissenschaftlichen Forschung erlaubt. Die Vervielfältigung muss also einem höheren Erkenntnisgewinn dienen, der einen Fortschritt für die Wissenschaft bedeutet. Eine Plagiatsüberprüfung beabsichtigt aber keinen höheren Erkenntnisgewinn, sondern die Aufdeckung von Täuschungsversuchen. Damit ist die Schranke des § 60d UrhG ebenfalls nicht ausreichend zur Rechtfertigung des einschlägigen Softwarebetriebes.

Neben den Schranken kommt noch die Erlaubnis des Urhebers in Frage. Eine solche kann ohne Vertrag durch eine simple Einwilligung geschehen oder, vertraglich abgesichert, durch eine explizite Einräumung von Nutzungsrechten. Im Rahmen der Kontrolle von Hochschularbeiten kommt sogar eine konkludente Einwilligung in Betracht. Konkludent ist eine Einwilligung, wenn sie erfolgt, ohne dass eine explizite Erklärung abgegeben wurde. Umgesetzt würde dies beispielsweise durch einen Hinweis auf die Plagiatsüberprüfung mittels Software in der Prüfungsordnung der jeweiligen Hochschule. So ist den Prüflingen bewusst, dass eine Überprüfung stattfindet, wenn sie ihre Arbeit einreichen. Eine Nutzungsrechteeinräumung ist etwas aufwendiger. Hier muss eine vertragliche Auseinandersetzung stattfinden. Der Prüfling müsste der Hochschule explizit die Nutzungsrechte einräumen, welche zur Plagiatsüberprüfung notwendig sind, also insbesondere das Recht zur Vervielfältigung. So erscheint die konkludente Einwilligung die praktikable Variante. Allerdings ist zu beachten, dass diese Einwilligung angefochten werden kann. Eine solche Anfechtung kommt insbesondere dann in Betracht, wenn die Einwilligung unter dem Druck einer widerrechtlichen Drohung zustande gekommen ist. Eine solche wird für den beschriebenen Fall, dass eine schlichte Plagiatsüberprüfung stattfindet, wohl nicht vorliegen. Auch wenn bis zum gewissen Grad durch den Hinweis in der Prüfungsordnung ein Zwang zur Einwilligung vorliegt, so ist diese Überprüfung auf Plagiate gerade zur Einhaltung der „guten wissenschaftlichen Lehre“ erforderlich und damit nicht widerrechtlich. Hinzu kommt, dass die Studierenden im Lichte der prüfungsrechtlichen Chancengleichheit selbst ein Interesse an einer Plagiatsüberprüfung haben.

Etwas Anderes kann dann gelten, wenn über die Plagiatsüberprüfung hinaus eine Archivierung der Arbeiten zum zukünftigen Abgleich mit Arbeiten erfolgen soll. Ein solches Vorgehen ist durch die „Grundsätze guter wissenschaftlicher Arbeit“ nicht indiziert und für den Prüfling nicht erwartbar. Um trotzdem eine Archivierung der Arbeiten durchzuführen und nicht dem Risiko einer Anfechtung ausgesetzt zu sein, verbleibt damit nur die Möglichkeit einer expliziten Nutzungsrechteeinräumung. Eine solche kann zum Beispiel durch Anhängen einer entsprechenden Vereinbarung an eine Prüfungsarbeit erfolgen.

IV. Datenschutzrechtliche Probleme

Bei dem Einsatz der Plagiatsüberprüfungssoftware werden auch Daten wie Namen, Adressen, Handschriften und ähnliches verarbeitet. Hierbei handelt es sich um personenbezogene Daten. Damit ist auch der Schutzbereich der

Datenschutz-Grundverordnung (DSGVO) eröffnet. Die Verarbeitung bedarf einer Rechtfertigung. In Frage kommen vorliegend eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO und die Aufgabenerfüllung im öffentlichen Interesse nach Art. 6 Abs. 1 lit. e DSGVO.

Eine datenschutzrechtliche Einwilligung ist zum einen gesondert einzuholen und kann zum anderen jederzeit ohne Angabe von Gründen widerrufen werden. Dementsprechend attraktiver erscheint die Rechtfertigung der Verarbeitung über Art. 6 Abs. 1 lit. e DSGVO. Das öffentliche Interesse ist im vorliegenden Fall durchaus in der Erhaltung der Grundsätze der guten wissenschaftlichen Lehre zu sehen. Wie soeben festgestellt, kann damit aber rechtssicher nur die Verarbeitung personenbezogener Daten im Zuge der Plagiatsüberprüfung als solcher und nicht der Archivierung gerechtfertigt werden. Außerdem zu beachten ist, dass es sich bei Art. 6 Abs. 1 lit. e DSGVO um eine Öffnungsklausel handelt, welche eine Konkretisierung des öffentlichen Interesses im konkreten Fall durch eine nationale Regelung fordert. Als eine solche Regelung kann schon der in den Hochschulgesetzen der Länder normierte Auftrag zur Kontrolle von Prüfungsarbeiten gelten. Die schlichte Plagiatsüberprüfung könnte auch noch konkreter in einer gesonderten Regelung normiert werden.

Um eine Archivierung der Prüfungsarbeiten zum zukünftigen Abgleich auch datenschutzrechtlich zu rechtfertigen, kommt nur die explizite Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO in Betracht. Zwar entsteht durch diese Modalität ein höherer Verwaltungsaufwand, eine andere rechtssichere Möglichkeit besteht nach hier vertretener Ansicht derzeit aber nicht.

V. Fazit und Auswirkungen für Hochschulen

Die Überprüfung von aufwendigen Arbeiten auf Plagiate mittels Software ist durchaus sinnvoll und liegt auch im Interesse der Studierenden. Bei der Durchführung ist darauf zu achten, dass ein entsprechender Vermerk in der Prüfungsordnung existiert, der in urheberrechtlicher Hinsicht eine konkludente Einwilligung der Prüflinge in Bezug auf die Plagiatskontrolle nach sich zieht. Aus Sicht des Datenschutzrechts ist auf eine konkretisierende Norm im nationalen Recht Wert zu legen und ein datensparsames Prozedere (bspw. durch Anonymisierung) einzuhalten. Eine Archivierung ist ohne Weiteres nur schwerlich rechtskonform umzusetzen. Hier empfiehlt sich die explizite Einholung von Nutzungsrechten sowie einer datenschutzrechtlichen Einwilligung. Beides sollte freiwillig geschehen.

Kleingedrucktes ganz groß: Klauseln für Klauseln

Das Vereinigte Königreich bietet nun eigene Standardvertragsklauseln

von Nicolas John

Der Austritt Großbritanniens aus der Europäischen Union (EU), der sog. Brexit, war schon öfter Thema in Beiträgen des DFN-Infobrief Rechts. Verwunderlich ist das nicht, denn die Abspaltung der Briten von der EU sorgt für einen grundlegenden Umbruch, der sich auch auf rechtlicher Seite in vielfältiger Weise zeigt. Für Hochschulen und Forschungseinrichtungen ist dies insbesondere im Datenschutzrecht zu spüren. Nachdem im Vereinigten Königreich derzeit eine kopierte Version der europäischen Datenschutz-Grundverordnung (DSGVO) in Form der UK General Data Protection Regulation (UK GDPR) gilt, hatte die Regierung von Boris Johnson Ende letzten Jahres einen Reformvorschlag zum britischen Datenschutzrecht vorgelegt, welcher grundlegende Pfeiler des bislang bekannten Datenschutzrechts anpassen soll.[1] Nun sind auch eigene britische Standardvertragsklauseln in Kraft getreten.

I. Hintergrund

Die Übermittlung von personenbezogenen Daten ist sowohl nach europäischen und damit derzeit auch nach britischen Regulierungen nur zulässig, wenn das angemessene Schutzniveau sichergestellt ist. Dieses kann vor allem durch das Vorliegen eines Angemessenheitsbeschlusses oder durch die Vereinbarung von Standardvertragsklauseln (Standard Contractual Clauses, kurz SCC) mit entsprechend einhergehenden technischen und organisatorischen Maßnahmen (TOM) geschehen.[2] Standardvertragsklauseln legen den Datenverarbeitenden bestimmte Verpflichtungen auf und sollen gleichzeitig die Rechte der Personen wahren, deren personenbezogene Daten übermittelt werden. Da nach dem Brexit durch die Übernahme der DSGVO in die UK GDPR dieselben Regelungen für Datenexporte gelten, müssen auch bei Exporten aus dem Vereinigten Königreich entsprechende Sicherheiten vorliegen. Maßgeblich ist dafür aber die UK GDPR, nicht die DSGVO. Diese britischen Regularien erlaubten zum Zeitpunkt des Brexit die Verwendung der damals geltenden alten EU-Standardvertragsklauseln (EU-SCC a.F.) für die Übermittlung personenbezogener Daten aus dem Vereinigten Königreich in Drittländer.

Doch die Europäische Kommission verabschiedete unter Berücksichtigung der Schrems-II-Entscheidung[3] neue, aktualisierte EU-Standardvertragsklauseln (EU-SCC).[4] Diese konnten jedoch keine Geltung im Vereinigten Königreich entfalten, da sie nach dem Brexit eingeführt wurden. Verantwortliche Personen konnten sich bei Datenübermittlungen aus dem Vereinigten Königreich daher nicht auf die neuen Standardvertragsklauseln berufen, solange das Vereinigte Königreich nicht die neuen EU-SCCs

1 Hierzu John, Data Wars: Episode IV – Eine neue Richtung, DFN-Infobrief Recht 4/2022.

2 Zu den Voraussetzungen für die Verwendung von SCCs: Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 8/2020; am Beispiel von Microsoft 365: John, New Schrems, new Me(crosoft), DFN-Infobrief Recht 2/2022.

3 Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 8/2020.

4 Tiessen, Santa Claus(e) is coming early, DFN-Infobrief Recht 8/2021; Wellmann, O ihr gnadenbringenden Standarddatenschutzklauseln, DFN-Infobrief Recht 12/2020.

oder einen anderen Datenübermittlungsmechanismus für sich selbst annahm.

Es bestand jedoch weiterhin die Möglichkeit, die alten europäischen Standardvertragsklauseln zu verwenden. Dies führte dazu, dass in der EU für Datenexporte in das Vereinigte Königreich die neuen Standardvertragsklauseln verwendet werden mussten, aber für Datenexporte aus dem Vereinigten Königreich die EU-SCC a.F. Die Folge war, dass Verträge, die Datenübertragungen sowohl aus dem Vereinigten Königreich als auch aus der EU beinhalten, mehrere Datenübertragungsmechanismen einhalten mussten. Zwischenzeitlich wurde seitens der EU ein Angemessenheitsbeschluss gemäß Art. 45 DSGVO für Großbritannien erlassen. Das Schutzniveau ist in Großbritannien somit als „der Sache nach gleichwertig" zu qualifizieren und personenbezogene Daten dürfen als Folge dieses Angemessenheitsbeschlusses ungehindert und ohne Ergreifen weiterer Maßnahmen i.S.d. Art. 46 ff. DSGVO transferiert werden. Der Angemessenheitsbeschluss der Kommission bezüglich Großbritannien besitzt vorläufig bis Juni 2025 Gültigkeit. Ebenso hat Großbritannien die Datenschutzvorschriften der Europäischen Union als angemessen anerkannt, was bedeutet, dass für Übermittlungen aus der EU in das Vereinigte Königreich und umgekehrt die Verwendung von SCCs nicht zwingend erforderlich ist.

Dennoch sah sich das UK Information Commissioner's Office (ICO) zum Entwurf neuer Standardvertragsklauseln durch das International Data Transfer Agreements (IDTA)[5] und eines Addendums[6] für das Vereinigte Königreich veranlasst. Grund hierfür war die Diskrepanz zwischen den EU-SCC und den im Vereinigten Königreich anerkannten EU-SCC a.F., sowie die Tatsache, dass die EU-SCC a.F. nicht alle Bestimmungen der UK GDPR berücksichtigten. Außerdem erging das Urteil in der Sache Schrems II noch vor dem Brexit. Das Vereinigte Königreich war daher verpflichtet, die Bestimmungen aus dem Urteil umzusetzen. Diese mögliche Angreifbarkeit der EU-SCC a.F. stellte eine Unsicherheit dar, die mit dem neuen IDTA nun beseitigt werden soll.

II. Die neuen Standardvertragsklauseln in Großbritannien

Am 21. März 2021 traten das IDTA und das UK Addendum nun in Kraft. Verantwortliche können entweder das IDTA oder das UK Addendum als Übermittlungsmechanismus nutzen, um gemäß Art. 46 UK GDPR „angemessene Garantien" für personenbezogene Daten zu bieten, wenn diese aus dem Vereinigten Königreich in Länder übermittelt werden, die nicht unter die Angemessenheitsvorschriften des Vereinigten Königreichs fallen.

1. Inhalt

Das IDTA und das UK Addendum sind zwei getrennte Datenübertragungsmechanismen, die Verantwortliche nutzen können. Während das IDTA eine eigene britische Form der europäischen SCCs ist, stellt das UK Addendum eine Ergänzung zu den geltenden EU SCCs dar. Verantwortliche können frei entscheiden, ob sie das IDTA oder das UK Addendum verwenden.

a. IDTA

Das IDTA funktioniert auf eigenständiger Basis und ist im Wesentlichen mit den EU SCCs vergleichbar. Es handelt sich um eine Muster-Vereinbarung, die für Übermittlungen in und aus dem Vereinigten Königreich verwendet werden soll.
Das IDTA besteht aus vier Teilen: Der erste Teil umfasst vier Tabellen, welche Informationen über die Parteien, die übermittlungsspezifischen Details, die datenspezifischen Informationen und die Sicherheitsanforderungen enthalten. Im zweiten Teil können die Parteien zusätzliche Schutzklauseln einfügen, wenn zusätzliche Maßnahmen erforderlich sind. Im dritten Teil können zusätzliche Handelsklauseln eingefügt werden, wenn es keine Vereinbarung zum IDTA gibt. Abschließend enthält der vierte und letzte Teil des IDTA wie die EU SCCs zwingende Klauseln, die in den Datenexportvertrag aufgenommen werden müssen. Die Bestimmungen des IDTA ähneln damit weitgehend denen der EU-SCC, jedoch ergeben sich auch einige Unterschiede.

5 UK Information Commissioner's Office, International Data Transfer Agreement, abrufbar unter https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf (zuletzt abgerufen am 08.04.2022).

6 UK Information Commissioner's Office, International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, abrufbar unter https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf (zuletzt abgerufen am 08.04.2022).

Der Anwendungsbereich des IDTA ist weiter als der der EU SCCs und kann in vielfältigeren Übermittlungssituationen eingesetzt werden. So sind z. B. Übermittlungen von Unterauftragsverarbeitern an Auftragsverarbeiter möglich, während die EU-SCCs solche Übermittlungen nicht vorsehen.

Unabhängig davon, ob das IDTA oder das UK Addendum als Übermittlungsmechanismus im Rahmen der UK GDPR verwendet wird, muss vor jeder Übermittlung ein „Transfer Risk Assessment" durchgeführt werden (Section 16; 16.1.1). Dies ist mit der Risikoprüfung des Datenschutzniveaus vergleichbar, welcher bei der Verwendung der aktuellen EU-SCCs erforderlich ist.

Sollten die Vertragsparteien schon eine andere Vereinbarung geschlossen haben, erlaubt das ITDA die Einbeziehung der Bedingungen dieser Vereinbarung, sofern die im Rahmen des IDTA gewährten Rechte nicht beeinträchtigt werden. Teil 2 des IDTA (Extra Protection Clauses) ermöglicht es zudem, dass alle zusätzlichen Garantien oder Maßnahmen, die gemäß Schrems II und den damit verbundenen Empfehlungen des Europäischen Datenschutzausschusses zu zusätzlichen Maßnahmen erforderlich sind, im IDTA gesondert aufgeführt werden können.

Für Datenimporteure, also den Datenverarbeitenden, welche personenbezogene Daten aus einem Drittland im Vereinigten Königreich empfangen, vereinfachen sich die Vorgaben teilweise: Zwar müssen sie gegenüber ihren Vertragspartnern, den Exporteuren (also den Datenverarbeitenden, welche die personenbezogene Daten an den Importeur senden) weiterhin angemessenen Aufwand betreiben, um über lokale Gesetze und Praktiken zu informieren, aber sie müssen nicht mehr sicherstellen, dass diese vollständig sind (Section 14; 14.2). Die Exporteure sind dagegen weiterhin verpflichtet, den betroffenen Personen Informationen über den Importeur mitzuteilen. Allerdings ist dies nur in Fällen erforderlich, in denen es dem Importeur nicht zumutbar ist, diese Informationen selbst zu Verfügung zu stellen (Section 11; 11.2.3).
Weiterhin enthält das IDTA die Verpflichtung für (Unter-)Auftragsverarbeiter, den Exporteur über Verletzungen des Schutzes personenbezogener Daten im Zusammenhang mit den übermittelten Daten zu informieren (Section 15; 15.2).
Außerdem enthält das IDTA Klauseln, die es den Parteien ermöglichen, das IDTA zu aktualisieren. Insbesondere ist eine automatische Aktualisierung des IDTA für den Fall vorgesehen, dass das ICO eine überarbeitete Version veröffentlicht (Section 5).
Ein Unterschied zu den EU SCC zeigt sich auch in der praktischen Verwendbarkeit: Das IDTA kann Datenübermittlungen rechtfertigen, wenn der Importeur ebenfalls der UK GDPR unterliegt. In den EU SCCs ist dies gemäß Erwägungsgrund 7 im Rahmen der europäischen Standardvertragsklauseln fraglich.

b. UK Addendum

Das UK Addendum hingegen funktioniert als Erweiterung zu den EU SCC: Es ergänzt diese so, dass sie auch für Übermittlungen aus dem Vereinigten Königreich verwendet werden können. Die Anpassungen betreffen insbesondere die richtige Benennung britischer Datenschutzvorschriften und Begriffsbestimmungen. Gerade in der Praxis kann diese Variante zu einer schnellen Umstellung der Verträge verhelfen.
Außerdem statuiert das UK Addendum, dass im Falle eines Konflikts zwischen den EU-SCC und dem UK Addendum das UK Addendum bei Übermittlungen nur dann Vorrang hat, wenn die Klauseln der EU SCC nicht mehr Schutz für die betroffenen Personen bieten. Demnach gelten die Klauseln, welche das höhere Schutzniveau bieten (Section 10).

2. Übergangsfristen

Das IDTA und das UK Addendum sind zwar bereits im März 2022 in Kraft getreten, in Neuverträge müssen sie jedoch erst ab 21. September 2022 verpflichtend eingebunden werden.
Vereinbarungen, die bis dahin abgeschlossen werden, dürfen auch weiterhin auf die bisherigen EU SCC a.F. gestützt werden und bleiben bis März 2024 gültig. Erst nach Ablauf dieser Frist müssen auch in diese Vereinbarungen das IDTA oder das UK Addendum eingebunden sein.

III. Fazit und Auswirkungen auf Hochschulen und Forschungseinrichtungen

Die Thematik ist vor allem für Hochschulen und Forschungseinrichtungen relevant, welche personenbezogene Daten mit Einrichtungen aus dem Vereinigten Königreich austauschen. Aufgrund der Übergangsfristen ist keine sofortige Änderung erforderlich. Aber auch nach Ablauf der Übergangsfrist kann weiterhin wegen der Angemessenheitsbeschlüsse von Kommission und UK der Datenaustausch ohne weiteres stattfinden.

Sollten doch SCCs verwendet werden, ist darauf zu achten, dass für Exporte aus der EU nur die EU SCCs den Datenexport rechtfertigen können. Das IDTA entspricht nicht den SCCs im Sinne der DSGVO. Umgekehrt kann bei Exporten aus dem Vereinigten Königreich mit Hilfe des Addendums auf die aktuellen EU-SCCs zurückgegriffen werden. In der Praxis dürfte das die einfachere Lösung sein, vor allem bei schon bestehenden Vereinbarungen, welche die EU-SCCs zur Basis haben.

Doch mit Blick auf die Pläne der britischen Regierung werden in den kommenden Jahren weitere Änderungen im Datenschutzrecht auf beide Seiten zukommen.[7] Sollten die Angemessenheitsbeschlüsse nach einer neuen Evaluierung des Datenschutzniveaus nicht verlängert werden, werden verantwortliche Personen auf Exportmechanismen der SCC zurückgreifen müssen. In diesem Fall ist die Erforderlichkeit von SCCs genau zu prüfen und als Grundlage für Exporte entsprechend heranzuziehen.

7 Im Detail hierzu: John, Data Wars: Episode IV – Eine neue Richtung, DFN-Infobrief Recht 4/2022.

Kurzbeitrag: Benutzung auf eigene Gefahr - Betreiber haften für ihre Nutzer!

Der BGH ändert seine Rechtsprechung zur urheberrechtlichen Haftung von Plattformen

von Owen Mc Grath

Anfang Juni hat der Bundesgerichtshof (BGH) seine Rechtsprechung zur Haftung von Plattformen für Urheberrechtsverstöße angepasst. Die einschlägigen Urteile befassten sich mit der Haftung der Betreiber von Internetsharehosting-Diensten, wie YouTube, für Urheberrechtsverletzungen, welche von Nutzern der Plattformen auf diesen begangen wurden.

I. Die Rechtsprechung

In den letzten Jahren vertrat der BGH die Auffassung, dass Plattformbetreiber für Verstöße gegen das Urheberrecht, welche von ihren Nutzern in Verwendung ihrer Plattform begangen wurden, nur als sogenannte Störer haften. Störer schulden keinen Schadensersatz, sondern nur Beseitigung und Unterlassung.[1] Diese Einschätzung wurde nun revidiert. In mehreren Verfahren urteilte der BGH, dass Plattformbetreiber durchaus als Täter und somit auch auf Schadensersatz verklagt werden können.

Zur Umkehr der Rechtsprechung kam es unter anderem auch dadurch, dass der BGH dem Gerichtshof der Europäischen Union (EuGH) mehrere Fragen zur Bewertung der Haftung vorgelegt hat. Dieser entschied, dass ein Plattformbetreiber selbst eine öffentliche Wiedergabe von rechtsverletzenden Inhalten vornimmt und damit Täter ist, wenn er „weiß oder wissen müsste, dass Nutzer über seine Plattform im Allgemeinen geschützte Inhalte rechtswidrig öffentlich zugänglich machen".[2] Um der direkten Haftung zu entgehen muss der Betreiber „die geeigneten technischen Maßnahmen ergreif[en], die von einem die übliche Sorgfalt beachtenden Wirtschaftsteilnehmer in seiner Situation erwartet werden können, um Urheberrechtsverletzungen auf dieser Plattform glaubwürdig und wirksam zu bekämpfen". Der Gerichtshof konkretisiert weiter, „dass die allgemeine Kenntnis des Betreibers von der rechtsverletzenden Verfügbarkeit geschützter Inhalte auf seiner Plattform für die Annahme einer öffentlichen Wiedergabe des Betreibers nicht genügt". Etwas Anderes gelte aber dann, wenn der Betreiber von Rechteinhabern über die Verstöße in Kenntnis gesetzt wurde und nicht unmittelbar handle. Eine weitere Einordnung als Täter trifft den Betreiber außerdem, wenn „er ein Geschäftsmodell gewählt hat, das die Nutzer seiner Plattform dazu anregt, geschützte Inhalte auf dieser Plattform rechtswidrig öffentlich zugänglich zu machen". Plattformbetreiber können danach durchaus nicht nur als Störer, sondern auch als Täter gelten. Schadensersatzansprüche gelten dann auch gegenüber den Betreibern. Eine Ausnahme der Haftung gilt aber für den Fall, dass geeignete technische Maßnahmen zur Verhinderung von Urheberrechtsverletzungen getroffen wurden, auf Hinweise zu Urheberrechtsverstößen umgehend reagiert wird und ein Geschäftsmodell gewählt wird, welches keine Urheberrechtsverletzungen fördert.

II. Bedeutung für Hochschulen und wissenschaftliche Einrichtungen

Für Hochschulen und wissenschaftliche Einrichtungen ist die Anpassung der Rechtsprechung aus zwei Perspektiven interessant. Zum einen ist bei Betrieb einer entsprechenden Plattform

1 Zur Störerhaftung: Tiessen, Wenn zwei sich freuen, haftet der Dritte, DFN-Infobrief Recht 5/2019.

2 Alle direkten Zitate aus: Pressemitteilung des BGH Nr. 080/2022.

darauf zu achten, selbst nicht in die Haftung zu geraten. Auf der anderen Seite ist als Rechteinhaber gegebenenfalls auch der Plattformbetreiber bei Urheberrechtsverletzungen in Haftung zu nehmen.
Mit Anpassung der Rechtsprechung durch den BGH ist in nächster Zeit auch eine Anpassung in niedrigeren Instanzen zu erwarten.

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

Podcast der Forschungsstelle Recht im DFN

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: https://anchor.fm/fsr-dfn