Haftungsrisiko „Webseite“: Vorsicht beim Einsatz von US - Dienstleistern

Dr. Markus Andrees

„Abschalten oder weiter nutzen?“ Vor dieser Frage stehen Betreiber von Webseiten häufig, wenn sie Stellungnahmen der Datenschutzaufsichtsbehörden zu in der Praxis weit verbreiteten Tools von IT-Dienstleistern aus den USA lesen. Dass diese Frage künftig noch mehr an Bedeutung gewinnen wird, lässt sich anknüpfend an ein Urteil des LG München I vom 20. Januar 2022 (Az. 3 O 17493/20) veranschaulichen.

I. Hintergrund der Entscheidung

Hintergrund der Entscheidung war folgende „alltägliche“ Situation: Ein Nutzer hat die Webseite des späteren Beklagten besucht und dabei festgestellt, dass der vom US-Anbieter Google betriebene Dienst „Google Fonts“ in die Seite eingebunden war. Über dieses Tool werden Schriftarten angeboten, die man für eine ansprechende Gestaltung der eigenen Webseite nutzen kann. Besonders einfach ist dies, wenn man sich als Webseitenbetreiber für die Variante entscheidet, einen HTML-Code in die eigene Webseite einzubinden, der bei Aufruf der Webseite eine Verbindung zum Server von Google aufbaut und die benötigte Schriftart in Sekundenbruchteilen nachlädt.

Dieser technisch unauffällige Vorgang ist datenschutzrechtlich relevant, weil der Verbindungsaufbau zum Server von Google mit einer Übertragung der IP-Adresse des Webseitenbesuchers einhergeht. Dass es sich bei einer dynamischen IP-Adresse um ein personenbezogenes Datum des Nutzers handelt, ist mittlerweile gefestigte Rechtsprechung. Für deren Übertragung an einen Dienstleister wie Google benötigt der Webseitenbetreiber eine datenschutzrechtliche Rechtfertigung. Eine solche konnte der Webseitenbetreiber jedoch nicht vorweisen. Folgerichtig ging das Gericht von einem Datenschutzverstoß aus und gab der auf Unterlassung der Übermittlung der IP-Adresse des Klägers gerichteten Klage statt.

II. Betreiber muss Schadenersatz zahlen

Dabei blieb das Gericht allerdings nicht stehen. Als „Anschauungsmaterial“ für die Praxis dient das Urteil gerade deshalb, weil dem Kläger zusätzlich Schadensersatz zugesprochen wurde. Das LG München I hat sich damit einer Strömung in der Rechtsprechung angeschlossen, die Art. 82 DS-GVO als Rechtsgrundlage für immateriellen Schadensersatz weit versteht. Wenn ein Nutzer – wie in diesem Fall angenommen – die Kontrolle schon über ein personenbezogenes Datum verliere (und dies auch noch an ein „datensammelfreudiges“ Unternehmen), rechtfertige das daraus resultierende „Unwohlsein“ beim Kläger eine Verurteilung zur Zahlung von Schadensersatz. Nur so könnten die vom Gesetzgeber angestrebten Ziele der Sanktion und Prävention erreicht werden.

Ob sich diese weite Interpretation des Schadensersatzes in der Rechtspraxis durchsetzt, wird sich in den kommenden Monaten zeigen. Der EuGH ist in mehreren Vorabentscheidungsverfahren zur Klärung der Frage aufgerufen, wie hoch die Voraussetzungen für einen Schadensersatzanspruch anzusetzen sind. Bislang waren die deutschen Zivilgerichte mehrheitlich eher zurückhaltend, wenn Kläger anknüpfend an rechtswidrige Datenverarbeitungen „Schmerzensgeld“ verlangt haben. Nur wenn der Kläger einen Schaden darlegen könne, der eine gewisse Erheblichkeit aufweise, könne überhaupt Geldersatz verlangt werden. Die deutschen Arbeitsgerichte zeigten sich hingegen in der Regel großzügiger. Sie sprachen – ebenso wie hier das LG München I – Klägern eine Entschädigung zu, selbst wenn es sich um Datenschutzverstöße mit bloß subjektiven und kaum messbaren Folgen handelte.

III. Folgen für die Praxis

Unter Berücksichtigung der inhaltlichen Schwere und der Dauer der Rechtsverletzung hielt das Landgericht München I zur Kompensation des klägerischen „Unwohlseins“ einen Betrag in Höhe von EUR 100,00 für angemessen. Isoliert betrachtet, dürfte diese Summe für einen Webseitenbetreiber nicht allzu schmerzhaft sein. Bedeutung erlangt das Urteil allerdings dadurch, dass es einen künftig häufiger zu erwartenden Konflikt vorzeichnet: Jeder beliebige Nutzer kann gezielt Webseiten mit datenschutzrechtlich „kritischen“ Diensten suchen, eine unzulässige Verarbeitung seiner eigenen personenbezogenen Daten durch den Webseitenbetreiber auslösen und anschließend dafür Geldersatz verlangen.

1. Handlungsoptionen für Betreiber

Dieses Risiko kann der Webseitenbetreiber selbstverständlich minimieren, indem er sich an das Datenschutzrecht hält. Der Beklagte hätte etwa eine von Google ebenfalls angebotene Variante wählen und damit den gleichen Effekt erzielen können. Hätte er die gewünschte Schriftart heruntergeladen und dann vom lokalen Rechner in die Webseite eingebunden, wären keine IP-Adressen von Nutzern der Webseite an Server von Google übertragen worden. Eine datenschutzrechtliche Problematik hätte es so nicht gegeben.

Die weitere denkbare Variante, sich eine Einwilligung vom Nutzer erteilen zu lassen, stünde hingegen aus Rechtsgründen auf „wackeligem" Fundament. Eine Einwilligung könnte zwar die Verarbeitung der IP-Adresse legitimieren. Ein Datentransfer in Länder mit einem geringeren Datenschutzniveau als in der EU – also auch in die USA – ist aber nur unter zusätzlichen strengen Voraussetzungen zulässig. Seit einem EuGH-Urteil aus dem Sommer 2020 (vgl. Legal Update vom 17. Juli 2020) besteht für Datentransfers in die USA im Kern nur noch die Möglichkeit, mit dem Empfänger vertragliche Schutzvorkehrungen abzuschließen, die das individuelle Risiko berücksichtigen müssen (dazu Legal Update vom 18. November 2020). Die ebenfalls in der DS-GVO vorgesehene Alternative, die Einwilligung des Betroffenen ausdrücklich auf die Übermittlung der Daten in die USA zu erstrecken, ist demgegenüber eher theoretischer Natur. Erst kürzlich wurde diese Vorgehensweise von den Datenschutzaufsichtsbehörden als absolute Ausnahme eingestuft, die regelmäßig wiederkehrende Datenübermittlungen in großem Umfang – wie im Fall des LG München I – nicht rechtfertigen könne.

2. Risikoabwägung

Unter Berücksichtigung dieser Handlungsoptionen wird die Herausforderung deutlich, vor der Betreiber von Webseiten stehen: Häufig gibt es nämlich keine Variante eines Tools von einem US-Dienstleister, die ohne Verbindungsaufbau zu einem in den USA befindlichen Server die gewünschte Leistung erbringt. Falls doch, ist diese Alternativlösung regelmäßig aufwändig zu implementieren und verringert ggf. sogar den Nutzerkomfort.

Es bleiben dann nur noch zwei Alternativen: Einerseits könnte der Webseitenbetreiber versuchen, die vertraglichen Schutzvorkehrungen für eine datenschutzkonforme Nutzung des Tools mit dem Anbieter zu vereinbaren. Andererseits könnte der Webseitenbetreiber vollständig auf das Tool verzichten.

Ersteres ist jedoch in der Praxis kaum realistisch. Anbieter wie Google zeigen nur geringes Interesse an individuell auszuhandelnden Verträgen, durch welche sie sich dem europäischen Datenschutzrecht unterwerfen würden. Letzteres kommt wiederum regelmäßig nicht in Betracht, da der Betreiber ohne das jeweilige Tool Qualitätseinbußen auf der eigenen Webseite hinnehmen müsste.

Dieses Dilemma lösen Webseitenbetreiber in der Praxis häufig im Rahmen einer Risikoabwägung. In der Hoffnung, dass die fehlende datenschutzkonforme Übermittlung personenbezogener Daten in die USA – wegen der bekannten Überlastung der Datenschutzbehörden – nicht auffällt, entscheiden sich zahlreiche Webseitenbetreiber für die (Weiter-)Nutzung von Tools, die von US-Dienstleistern angeboten werden.

IV. Fazit: Neubewertung des Risikos

Als Fazit lässt sich festhalten, dass die Einbindung zahlreicher beliebter Tools von US-Anbietern in Webseiten mit datenschutzrechtlichen Risiken verbunden ist. Diese sollten, wie die Entscheidung des LG München I eindrucksvoll bestätigt, nicht unterschätzt werden:

„Findige Nutzer" werden, angetrieben von Entscheidungen wie der des LG München I, vermutlich verstärkt die Chance suchen, mit relativ wenig Aufwand eine lukrative Einnahmequelle zu generieren. Dabei dürfte ihnen entgegenkommen, dass im Markt eine Vielzahl von US-Tools verbreitet ist, die ähnlich wie „Google Fonts" zumindest die IP-Adresse (und häufig noch weitere personenbezogene Daten) an Server in den USA übermitteln. Diese lassen sich für einen Besucher einer Webseite regelmäßig auch ohne allzu großes technisches Fachwissen identifizieren.

Zwar besteht bei einer Mehrzahl der deutschen Zivilgerichte noch eine erkennbare Tendenz, Klägern kein Schmerzensgeld zuzusprechen, wenn in datenschutzrechtswidriger Weise personenbezogene Daten an einen Empfänger in den USA übermittelt werden, ohne dass dies zu Schäden von gewisser Schwere führt. Das Urteil des LG München I zeigt allerdings, dass man sich auf diese Zurückhaltung nicht verlassen sollte.

Hinweis

Dieser Überblick dient ausschließlich der allgemeinen Information und kann konkreten Rechtsrat im einzelnen Fall nicht ersetzen. Sprechen Sie bei Fragen bitte Ihren gewohnten Ansprechpartner bei GÖRG bzw. den Autor Markus Andrees unter +49 221 33660 244 oder mandrees@goerg.de an. Informationen zum Autor finden Sie auf unserer Homepage www.goerg.de.

Unsere Standorte

GÖRG Partnerschaft von Rechtsanwälten mbB

BERLIN
Kantstraße 164, 10623 Berlin
Tel. +49 30 884503-0, Fax +49 30 882715-0

FRANKFURT AM MAIN
Ulmenstraße 30, 60325 Frankfurt am Main
Tel. +49 69 170000-17, Fax +49 69 170000-27

HAMBURG
Alter Wall 20 – 22, 20457 Hamburg
Tel. +49 40 500360-0, Fax +49 40 500360-99

KÖLN
Kennedyplatz 2, 50679 Köln
Tel. +49 221 33660-0, Fax +49 221 33660-80

MÜNCHEN
Prinzregentenstraße 22, 80538 München
Tel. +49 89 3090667-0, Fax +49 89 3090667-90