EUGH ENTSCHEIDET: EINWILLIGUNG FÜR SOCIAL PLUGINS UND TRACKING ERFORDERLICH

Wer für eine Website Social Plugins von Facebook nutzt, braucht hierfür eine vorherige, ausdrückliche Einwilligung seiner Nutzer und ist gemeinsam mit Facebook für die Datenverarbeitung verantwortlich. Das hat der EuGH am 29.7.2019 im Rechtsstreit zwischen der Fashion ID GmbH & Co. KG und der Verbraucherzentrale Nordrhein-Westfalen entschieden (Aktenzeichen: C-40/17). Dabei handelt es sich um eine Grundsatzentscheidung, denn die gerichtlichen Vorgaben gelten für Websites und Apps sowie für fast alle Social Plugins und Trackingtools.

Worum geht es bei „Fashion ID"?

Fashion ID, ein Online-Händler für Modeartikel, band in seine Website das Social Plugin „Gefällt mir" ein („Like Button"). Mit jedem Aufruf der Website wurden personenbezogene Daten jedes Nutzers der Website an Facebook in Irland übermittelt, ohne dass die Nutzer einwilligten, hierüber den gesetzlichen Vorgaben entsprechend informiert wurden und unabhängig davon, ob die Nutzer einen Account bei Facebook hatten oder nicht. Die Verbraucherzentrale Nordrhein-Westfalen nahm Fashion ID deshalb vor dem LG Düsseldorf auf Unterlassung in Anspruch und gewann teilweise (Urteil v. 9.3.2016 – 12 O 151/15). Hiergegen ging Fashion ID vor dem OLG Düsseldorf in Berufung, welches den EuGH um Klärung verschiedener Rechtsfragen bat (Beschluss v. 19.1.2017 – I-20 U 40/16).

Was hat der EuGH entschieden?

Der EuGH hat mit seinem Urteil mehrere Entscheidungen gleichzeitig getroffen:

- Verbraucherschutzverbände sind zur Geltendmachung von Datenschutzverletzungen jedenfalls nach der alten Datenschutzrichtlinie klagebefugt; ob das auch für die DS-GVO gilt wurde nicht entschieden.
- Wer das Plugin eines Dritten (hier: Facebook als Plugin-Anbieter) in seine Website einbindet, hieraus einen wirtschaftlichen Vorteil z.B. durch Optimierung der eigenen Werbung erzielt und zu diesem Zweck mit dem Tool auf seiner Website personenbezogene Daten erhebt und diese an den Plugin-Anbieter übermittelt, geht eine gemeinsame Verantwortlichkeit mit dem Plugin-Anbieter gemäß Art. 26 DS-GVO ein (englisch „Joint Controllership"). Es genügt, wenn auf einer solchen abstrakten Ebene gemeinsam vom Website-Betreiber und Plugin-Anbieter über Zwecke und Mittel der Verarbeitung entschieden wird.
- Entscheidet der Plugin-Anbieter (hier: Facebook) anschließend allein, was mit den personenbezogenen Daten geschieht, ist für diese Weiterverarbeitung der Plugin-Anbieter eigenständig verantwortlich und der Website-Betreiber bleibt außen vor. Profitiert jedoch der Website-Betreiber von den Ergebnissen dieser Verarbeitung, z.B. weil ihm die Ergebnisse als aggregierte Auswertungen zur Verfügung gestellt werden, erstreckt sich die gemeinsame Verantwortlichkeit auch auf die Weiterverarbeitung durch den Plugin-Anbieter; das hat der EuGH bereits 2018 zu Facebook Fanpages entschieden (Urteil v. 5.6.2018 – C-210/16).
- Wird von einem Plugin ein Cookie auf dem Endgerät des Nutzers abgelegt oder werden vom Plugin (ggf. auch fremde) Cookies oder andere Informationen auf dem Endgerät ausgelesen, bedarf es hierfür einer vorherigen, ausdrücklichen Einwilligung des Nutzers (sog. Opt-in). Ein späterer Widerspruch (sog. Opt-out) ist nicht ausreichend. Der noch geltende § 15 Abs. 3 Telemediengesetz (TMG), der für pseudonymisierte Datenverarbeitungen insbesondere zu Werbezwecken eine Widerspruchslösung für ausreichend erachtet, ist damit europarechtswidrig und kann ab sofort nicht mehr als Rechtsgrundlage herangezogen werden.
- Die Einwilligung muss sich auf die gesamte gemeinsame Verarbeitung beziehen, also auf die Erhebung durch den Website-Betreiber und die anschließende Übermittlung an Facebook. Jeder gemeinsam Verantwortliche (englisch „Joint Controller") bedarf dabei einer eigenen Erlaubnis für die gemeinsame Verarbeitung. Anders als die Auftragsverarbeitung gemäß Art. 28 DS-GVO kennt die gemeinsame Verantwortlichkeit keine Privilegierung.
- Mit Beginn der Verarbeitung durch den Website-Betreiber, also bei Aufruf der Website, muss die Einwilligung eingeholt und eine gesetzeskonforme Datenschutzinformation gemäß Art. 13, 14, 21 DS-GVO erteilt werden. Zugleich müssen auch die besonderen Informationen gemäß Art. 26 Abs. 2 S. 2 DS-GVO über das in gemeinsamer

Verantwortlichkeit erfolgende Erheben und Übermitteln der Daten durch den Website-Betreiber an den Plugin-Anbieter zur Verfügung gestellt werden. Dies muss nach dem EuGH zwingend durch den Website-Betreiber geschehen.

Welche Bedeutung hat das Urteil für Website- und App-Betreiber?

Das Urteil bezieht sich konkret auf den Like-Button von Facebook und dessen Einbindung in Websites. Die gerichtlichen Vorgaben gelten aber für alle Plugins und Tools, bei denen die Voraussetzungen aus dem Urteil vorliegen. Sie sind auch nicht auf Websites beschränkt, sondern auf alle Telemedien anwendbar, insbesondere auf Apps:

- Das Plugin/Tool wird von einem Dritten angeboten.
- Das Plugin/Tool wird vom Anbieter in seine Website oder App eingebunden, um wie vom Plugin/Tool vorgesehen Informationen von den Nutzern der Website/App zu erlangen und diese Informationen an den Anbieter des Plugins/Tools zu übermitteln.
- Das Plugin/Tool speichert Informationen, insb. personenbezogene Daten, auf dem Endgerät des Nutzers der Website oder App, z.B. auf einem Smartphone, Tablet oder Notebook. Meist werden die Informationen in Cookies gespeichert. Alternativ reicht es aus, wenn das Plugin/Tool zwar keine Informationen auf dem Endgerät speichert, aber auf bereits auf dem Endgerät gespeicherte Informationen zugreift, z.B. auf Fremd-Cookies oder Angaben zum Endgerät, z.B. eine Device-ID.
- Der Anbieter des Plugins/Tools und der Betreiber der Website/App verfolgen mit dem Anbieten/Einbinden des Plugins/Tools gleichartige, in der Regel kommerzielle oder werbliche Zwecke und fördern wechselseitig deren Erreichung. Eine völlige Übereinstimmung oder Identität der Zwecke ist nicht erforderlich.

Erfasst sind damit neben dem Like-Button von Facebook nahezu alle Plugins der sozialen Netzwerke, aber auch das Facebook Pixel, das LinkedIn Insight-Tag, Analyse-Tools wie Google Analytics oder Heatmap Tools wie Hotjar. Ebenso fallen Tools darunter, die etwa zur Ermöglichung von Push-Funktionalitäten Geräte-Kennziffern (Device-IDs) oder andere Informationen von Endgeräten auslesen.

Aus dem Anwendungsbereich fallen nur solche Plugins/Tools heraus, bei denen eine der obigen Voraussetzungen nicht gegeben ist. Das ist insbesondere der Fall, wenn das Plugin/Tool keine Informationen auf dem Endgerät speichert und auch nicht auf bereits gespeicherte Informationen auf dem Endgerät zugreift, oder wenn ausschließlich der Website-/App-Betreiber die Informationen aus dem Plugin/Tool erhält, oder wenn die Informationen vom Anbieter des Plugins/Tools ohne Verfolgung eigener Zwecke ausschließlich unter der Kontrolle des Website-/App-Betreibers und damit als Auftragsverarbeitung gemäß Art. 28 DS-GVO vom Plugin-Anbieter verarbeitet werden. Werden Plugins/Tools auf einem eigenen Server ohne Zugriffsrechte für den Plugin-/Tool-Anbieter betrieben (z.B. das Analyse-Tool Matomo), entfällt zwar die gemeinsame Verantwortlichkeit, die Einwilligung muss vom Nutzer aber trotzdem eingeholt werden.

Was müssen Sie jetzt machen?

Folgende Punkte sollte jeder Website-/App-Betreiber jetzt prüfen:

- Welche Plugins/Tools werden für Ihre Website/App genutzt? Häufig ist dies nicht bekannt, weil ein IT-Dienstleister oder eine Agentur nach eigenem Ermessen Tools in die Website/App „eingebaut“ haben.
- Speichern die genutzten Plugins/Tools Informationen auf den Endgeräten Ihrer Nutzer, insbesondere in Cookies, und übermitteln diese Informationen an den Anbieter? Alternativ: Greifen die genutzten Plugins/Tools auf bereits auf dem Endgerät Ihrer Nutzer gespeicherte Informationen zu, die dann an den Anbieter des Plugins/Tools übermittelt werden?
- Verfolgen Sie als Website-/App-Betreiber mit der Nutzung der Plugins/Tools gleichartige Zwecke wie dessen Anbieter, insbesondere profitieren Sie von der Verarbeitung der mit dem Plugin/Tool erhobenen oder sonst verarbeiteten Informationen durch den Anbieter des Plugins/Tools?

Für jedes Plugin/Tool, für das die vorstehenden Fragen alle mit „ja" beantwortet werden, sind folgende Maßnahmen erforderlich:

- Schließen Sie mit dem Anbieter des Plugins/Tools eine Vereinbarung über die gemeinsame Verantwortlichkeit gemäß Art. 26 Abs. 1 S. 2 DS-GVO ab. Stellt der Anbieter keine solche Vereinbarung zur Verfügung und ist auch nicht bereit, eine von Ihnen vorgeschlagene Vereinbarung zu akzeptieren, ist die Nutzung des Plugins/Tools immer datenschutzrechtswidrig.
- Informieren Sie die Nutzer Ihrer Website/App über das Plugin/Tool und stellen dafür alle Datenschutzinformationen gemäß Art. 13, 14, 21 DS-GVO sowie ergänzend die Informationen zur gemeinsamen Verantwortlichkeit gemäß Art. 26 Abs. 2 S. 2 DS-GVO zur Verfügung. Das muss passieren, bevor es zur Speicherung von oder zum Zugriff auf Informationen auf dem Endgerät des Nutzers kommt. Das Fehlen der Informationen ist ein Datenschutzverstoß.
- Holen Sie vor Aktivieren des Plugins/Tools eine ausdrückliche Einwilligung (Opt-in) der Nutzer ein, die den Vorgaben insbesondere aus Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a) und Art. 7 DS-GVO entspricht. Dokumentieren Sie den von Ihnen hierfür implementierten Prozess sowie die technischen Vorgänge im Zusammenhang mit der Einholung der Einwilligung. Es dürfen erst dann Informationen auf dem Endgerät gespeichert oder von dort abgerufen werden, wenn die Einwilligung des Nutzers vorliegt. Das ist nur möglich, wenn beim ersten Aufruf der Website mit einem Cookie-Overlay oder einer speziellen Landingpage zunächst die Einwilligung abgefragt wird, bevor die Datenverarbeitungen beginnen. Soweit Social-Media-Plugins genutzt werden, kann alternativ eine 2-Klick-Lösung wie der Shariff aus dem Heise Verlag eingesetzt werden. Dann muss die Einwilligung erst mit dem Aktivierungs-Klick des Nutzers auf ein Plugin/Tool eingeholt werden. Ohne die vorherige, ausdrückliche Einwilligung ist die Nutzung des Plugins/Tools datenschutzrechtswidrig. Eine Widerspruchslösung (Opt-out) reicht nicht mehr aus.

Setzen Sie ein Plugin/Tool ein, ohne diese Maßnahmen umgesetzt zu haben, laufen Sie Gefahr, dass die Datenschutzaufsicht die weitere Nutzung untersagt und ggf. ergänzend eine Geldbuße gegen Sie verhängt wird. Zudem können Nutzer Ihrer Website und ggf. auch Mitbewerber rechtlich gegen Sie vorgehen.

Welche Fragen hat der EuGH (u.a.) nicht beantwortet?

Der EuGH hat verschiedene, kontrovers diskutierte Fragen nicht entschieden:

- Der EuGH hat sich nicht dazu geäußert, ob Mitbewerber zur Abmahnung von Datenschutzverletzungen berechtigt sind. Diese Frage wird von den Gerichten in Deutschland unterschiedlich beantwortet, sodass derzeit keine Rechtssicherheit besteht.
- Zu den Folgen einer gemeinsamen Verantwortlichkeit unter der DS-GVO gibt es keine Feststellungen. Das betrifft insbesondere Verantwortlichkeit und Haftung von Plugin-/Tool-Anbieter und Website-/App-Betreiber im Verhältnis zueinander sowie gegenüber den Nutzern und anderen Dritten. Auch zur gemäß Art. 26 Abs. 1 S. 2 DS-GVO möglichen Aufteilung der Datenschutzpflichten aus der DS-GVO zwischen den gemeinsam Verantwortlichen findet sich im Urteil nichts. Der EuGH stellt lediglich klar, dass sich eine zivilrechtliche Haftung der Beteiligten auch aus nationalem Recht ergeben kann und nicht allein aus der DS-GVO abzuleiten ist.
- Nicht entschieden hat der EuGH, wie in der Praxis der Nachweis der über die Website/App eingeholten Einwilligungen in die Nutzung der Plugins/Tools zur Erfüllung der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO und der Nachweispflicht aus Art. 7 Abs. 1 DS-GVO geführt werden kann. Ebenso wenig hat der EuGH festgelegt, wie im Detail das technische Verfahren zur Einholung der Einwilligung auszugestalten ist, wie die Einwilligung zu formulieren ist und wie die Möglichkeit zum Widerruf der Einwilligung durch den Nutzer ausgestaltet werden muss.
- Schließlich hat der EuGH keine Aussage zur Zulässigkeit sog. Cookie Walls getroffen. Cookie Walls schließen den Nutzer von einer Website/App aus, wenn die Einwilligung in die Nutzung der Plugins/Tools nicht erteilt

wird, oder verweisen den Nutzer alternativ auf ein inhaltlich reduziertes oder kostenpflichtiges Angebot. Während von der Datenschutzaufsichtsbehörde in Österreich solche Cookie Walls für zulässig erachtet werden, sieht die niederländische Datenschutzaufsicht darin einen Verstoß gegen das sog. Kopplungsverbot aus Art. 7 Abs. 4 DS-GVO und erachtet mit einer solchen Cookies Walls eingeholten Einwilligungen mangels Freiwilligkeit für unwirksam.

Wie können wir Sie unterstützen?

Es gibt viele konkrete Unterstützungsmöglichkeiten:

- Nennen Sie uns die von Ihnen für Ihre Website/App genutzten Plugins/Tools und wir prüfen zum Pauschalpreis, welche der Plugins/Tools eine Einwilligung und eine Vereinbarung zur gemeinsamen Verantwortlichkeit erfordern.
- Wir erstellen Ihnen für Ihre Website/App einschließlich der von Ihnen genannten Plugins/Tools zum Pauschalpreis eine den gesetzlichen Vorgaben entsprechende Datenschutz-Information („Datenschutzerklärung“) gemäß Art. 13, 14, 21 DS-GVO.
- Wir erstellen Ihnen für die von Ihnen genutzten Plugins/Tools eine datenschutzkonforme Einwilligungserklärung und stimmen mit Ihnen ab, wie diese Einwilligung in Ihre Website/App eingebunden werden kann. Dies erfolgt abhängig von Art und Anzahl der Plugins/Tools entweder zum Pauschalpreis oder wir unterbreiten Ihnen ein verbindliches Angebot.
- Wir prüfen zum Pauschalpreis, ob die vom Anbieter eines Plugins/Tools bereitgestellten Vereinbarungen zur gemeinsamen Verantwortlichkeit gemäß Art. 26 DS-GVO nebst den zugehörigen Datenschutz-Informationen den gesetzlichen Vorgaben entsprechen und von Ihnen abgeschlossen werden können, damit Sie das Plugin/Tool datenschutzkonform nutzen können.
- Benötigen Sie eine eigene Vereinbarung zur gemeinsamen Verantwortlichkeit nebst zugehörigen Datenschutz-Informationen, unterbreiten wir Ihnen ein verbindliches Angebot für deren Erstellung.

Wer sind Ihre Ansprechpartner?

Wenn Sie von uns im Datenschutz bereits beraten werden wenden Sie sich bitte an die/den Sie betreuende Rechtsanwältin/Rechtsanwalt. Nehmen Sie anderenfalls jederzeit gerne Kontakt zu einer/einem der folgenden Ansprechpartner/innen auf:

Sascha Kremer, Fachanwalt für IT-Recht, externer Datenschutzbeauftragter (TÜV), sascha.kremer@kremer-recht.de
Per Stöcker, Rechtsanwalt, Datenschutzbeauftragter (ECPC/Maastricht University und TÜV), per.stoecker@kremer-recht.de
Daniela Köhnlechner, Rechtsanwältin, Datenschutzbeauftragte (TÜV), daniela.koehnlechner@kremer-recht.de
Nadine Schneider, Rechtsanwältin, Datenschutzbeauftragte (TÜV), nadine.schneider@kremer-recht.de
Malte Dümeland, Rechtsanwalt, Datenschutzbeauftragter (TÜV), malte.duemeland@kremer-recht.de
Kristof Kamm, Rechtsanwalt, Datenschutzbeauftragter (TÜV), kristof.kamm@kremer-recht.de

Alle Ansprechpartner erreichen Sie unter 0221/27141874 und persönlich in der Brückenstraße 21, 50667 Köln (Innenstadt).

Wer sind KREMER RECHTSANWÄLTE?

KREMER RECHTSANWÄLTE ist eine auf Digitalisierungsberatung spezialisierte Sozietät und berät mit insgesamt vierzehn Rechtsanwältinnen und Rechtsanwälten ihre Mandanten und Auftraggeber, darunter DAX-Konzerne, KMU, Kreditinstitute und Finanzdienstleister jeglicher Größe, kirchliche Einrichtungen und Startups, hochspezialisiert an der Schnittstelle zwischen Technik und Recht. Die Sozietät hat in verschiedenen Branchen- und Dachverbänden an der Umsetzung der DS-GVO durch die jeweiligen Mitglieder mitgewirkt und selbst mehrere Großprojekte zur Umsetzung der DS-GVO erfolgreich geführt oder begleitet. KREMER RECHTSANWÄLTE wird u.a. im kanzleimonitor.de 2018/2019 als empfohlene Kanzlei im IT- und Datenschutzrecht geführt.