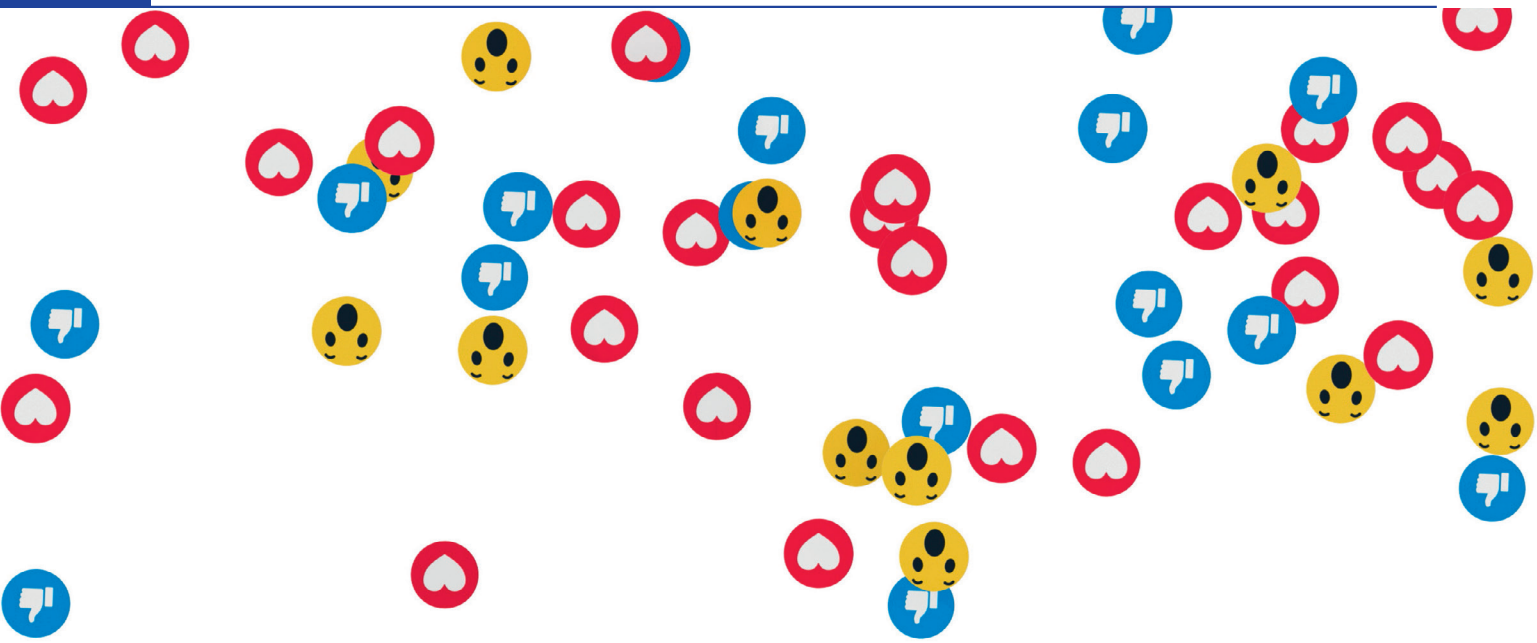

Dr. Martin Bahr

Die „Fashion ID“-Entscheidung des EuGH: Praktische Konsequenzen für alle Seitenbetreiber, die Social-Plug-ins oder externe Tracking-Tools einbinden

Eine aktuelle Gerichtsentscheidung des Europäischen Gerichtshofs (EuGH) vom Juli 2019 führt zu einer grundlegenden Änderung der Rechtslage bei der Einbindung von externen Tools wie Social-Plug-ins oder Tracking-Tools wie Google Analytics. Das Urteil wird – über kurz oder lang – massive Auswirkungen auf den Online-Bereich haben.
So wurde vor Kurzem bekannt, dass das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) gegen mehrere Webseiten-Betreiber ein Bußgeldverfahren betreibt, weil diese Google Analytics, Double Click und Criteo eingebunden haben.

DER AUTOR

Die **Kanzlei Dr. Bahr** *(http://www.Dr-Bahr.com)* ist auf den Bereich des Rechts der Neuen Medien und den gewerblichen Rechtsschutz (Marken-, Urheber- und Wettbewerbsrecht) spezialisiert. Unter Suchmaschinen-und-Recht.de betreibt sie seit 2005 ein eigenes Themenportal zur rechtlichen Dimension von Suchmaschinen.

A. Was beinhaltet die sog. „Fashion ID“-Entscheidung des EuGH?

Der Begriff „Fashion ID“ ist das Label, unter dem eine Unternehmens-Tochter von Peek & Cloppenburg seine Bekleidung verkauft. Das Unternehmen hatte auf seiner Webseite *Fashionid.de* den üblichen Like-Button von Facebook eingebunden. Bereits bei Aufruf der Webseite war das Tool aktiv.

Die Verbraucherzentrale NRW sah hierin einen Rechtsverstoß, da die Einbindung der Facebook-Erweiterung nicht datenschutzkonform erfolgte, und klagte. Die verklagte Firma hielt dagegen und argumentierte, dass sie gar nicht verantwortlich sei, da die Datenverarbeitung durch Facebook geschehe. Facebook sei also verantwortlich, so der Standpunkt.

Über Jahre zog sich die Auseinandersetzung hin, bis schließlich das OLG Düsseldorf dem Europäischen Gerichtshof (EuGH) den Sachverhalt vorlegte. Mitte Juli 2019[1] sprach der EuGH dann nun ein Machtwort.

Nach Meinung der EuGH-Richter ist die Beklagte für sämtliche Aktivitäten, die der Like-Button vornimmt, neben Facebook mit verantwortlich. Ein Webseiten-Betreiber kann sich somit nicht aus der Verantwortung stehlen und einfach auf Facebook verweisen.

Die Europa-Richter weisen darauf hin, dass

[1] EuGH, Urt. v. 29.07.2019 – Az. C-40/17 = Volltext unter https://openjur.de/u/2177461.html

hier eine sogenannte gemeinsame Verantwortlichkeit nach Art. 26 DSGVO vorliegt.

Praxis-Tipp:
Die meisten Leser werden von dem Begriff der gemeinsamen Verantwortlichkeit noch nie etwas gehört haben. Dies ist auch wenig verwunderlich, denn bis vor Kurzem führte dieser in der juristischen Welt ein Schattendasein.
Hingegen wird den meisten der Begriff „Auftragsdatenverarbeitung" (ADV) bzw. „Auftragsverarbeitung" (AVV) schon einmal über den Weg gelaufen sein. Nicht zuletzt aufgrund der am 25.05.2018 in Kraft getretenen DSGVO.
Bei der ADV gibt es den Auftraggeber und den Auftragnehmer, ein klares Über-Unter-Ordnungsverhältnis. So ist z. B. Auftragnehmer der Webhoster, bei dem der Webseiten-Betreiber, also der Auftragnehmer, seine Webseite liegen hat.
Bei der gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO gibt es hingegen kein solches Auftragsverhältnis. Beide Parteien stehen gleichberechtigt nebeneinander und kooperieren grundsätzlich auf Augenhöhe. Alles Weitere zur gemeinsamen Verantwortlichkeit finden Sie unter Punkt C.

B. Gelten die Aussagen nur für den Like-Button von Facebook?

Auch wenn sich die Entscheidung des EuGH formal nur auf den Like-Button von Facebook bezieht, gelten die Ausführungen grundsätzlich 1:1 für alle externen Tools, die ein Webseiten-Betreiber bei sich einbindet und die personenbezogene Daten übertragen.

Bedeutet im Klartext: alle Tracking-Tools à la Google Analytics, alle Retargeting-Instrumente (z. B. Criteo oder Double Click) oder Social-Plugins (z. B. Facebook, Instagram oder YouTube), die mindestens die IP-Adresse oder sonstige personenbezogene Daten des Surfers weitergeben.

Das Urteil ist damit eine kaum zu überschätzende Grundlagen-Entscheidung, die praktisch für jeden Webseiten-Betreiber in der einen oder anderen Weise relevant ist.

Nicht zuletzt auch deshalb, weil inzwischen bekannt wurde, dass das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) jetzt Ernst macht und gegen mehrere Webseiten-Betreiber ein Bußgeldverfahren betreibt, weil diese Google Analytics, Double Click und Criteo eingebunden haben.[2] Die Behörde vertritt den Standpunkt, dass ein Berufen auf die berechtigten Interessen nach Art. 6 Abs. 1 f) DSGVO nicht möglich sei, weil für die Abwägung die konkreten Umstände der Datenverarbeitung bei den Anbietern notwendig wäre. Dieses Wissen fehle dem Webseiten-Betreiber jedoch.

Ebenso hat das Bundesverwaltungsgericht[3] vor Kurzem entschieden, dass sich eine Aufsichtsbehörde aussuchen kann, ob sie gegen Facebook oder den Page-Betreiber vorgeht. Im Zweifel ist also der Seitenbetreiber dran und nicht der jeweilige Tool-Anbieter.

C. Praktische Konsequenzen: Ihre To-dos

Was muss ich nun nach der „Fashion ID"-Entscheidung genau unternehmen, um rechtskonform zu handeln?

Die Antwort ist relativ einfach, aber ernüchternd: Momentan können Sie rechtskonform keine Webseite betreiben, wenn Sie solche Tools eingebunden haben. Sie können jedoch versuchen, sich so gut wie möglich zu verhalten, um für den Fall der Fälle Ihren good will zu demonstrieren.

a) Abschluss einer Joint-Controllership-Vereinbarung

Wie unter Punkt A. erläutert, hat der EuGH festgestellt, dass zwischen dem Webseiten-Betreiber und dem Tool-Betreiber eine gemeinsame Verantwortlichkeit vorliegt. Demnach reicht hier ein ADV nicht mehr aus, sondern Sie müssen mit jedem einzelnen Anbieter eine derartige Vereinbarung schließen.

Praxis-Tipp:
Soweit ersichtlich bietet bislang lediglich Facebook für Fanpages eine solche Vereinbarung an. Nach Einschätzung der deutschen Datenschutzbehörden ist dieses Muster jedoch nicht ausreichend. Die meisten anderen Anbieter haben bis dato nicht reagiert und bieten keine vergleichbaren Dokumente an.
Zwar stellt die Datenschutzbehörde in Baden-Württemberg ein kostenloses Muster für eine Joint-Controllership-Vereinbarung zur Verfügung.[4] Es liegt aber auf der Hand, dass die großen ausländischen Tool-Anbieter keine solchen Individual-Vereinbarungen akzeptieren werden. Es bleibt abzuwarten, ob und wie Google & Co. auf diese Problematik reagieren werden.

Da eine solche Joint-Controllership-Vereinbarung aktuell praktisch mit keinem der Anbieter geschlossen werden kann, ist bereits aus formalen Gründen der Tool-Einsatz datenschutzwidrig.

b) Inhaltliche Probleme

Die Problemlage ist jedoch nicht nur formaler Natur, sondern betrifft vielmehr auch den Inhalt.

[2] Vgl. https://bit.ly/2lKvOZz
[3] BVerwG, Urt. V. 11.09.2019 – Az.: 6 C 15.18
[4] Vgl. https://bit.ly/2KOUYBZ
[5] Vgl. https://bit.ly/2hOWodN
[6] Vgl. https://www.lda.bayern.de/de/faq.html
[7] Vgl. https://www.lda.bayern.de/de/faq.html

aa. Einwilligungen unzureichend

Mancher Webseiten-Betreiber kommt auf die Idee, derartige Tools durch eine Einwilligung, die er bei einem User abfragt, zu legitimieren. Eines der bekanntesten Beispiele hierfür ist das Tool Shariff des Heise-Verlages.[5] Der Nutzer muss im Wege einer ausdrücklichen Zustimmung (sog. 2-Klick-Lösung) seine Einwilligung geben. Erst dann werden die Daten übermittelt. Eine andere Idee ist, den üblichen Cookie-Banner dem Aufruf einer Webseite vorzuschalten.

Beide Lösungen haben eines gemeinsam: Sie führen grundsätzlich nicht zur Rechtmäßigkeit. Denn damit eine Einwilligung wirksam ist, muss eine umfassende und transparente Information über Art, Inhalt und Umfang der Einwilligung vorausgehen. Da die meisten Tool-Anbieter diese Informationen nicht bereitstellen, kann somit auch der Webseiten-Betreiber seine Besucher hierüber nicht informieren.

Was in letzter Konsequenz nichts anderes bedeutet, als dass sowohl die 2-Klick-Lösungen als auch die Cookie-Banner schönes Beiwerk sind, aber nichts an der Rechtswidrigkeit ändern.

Praxis-Tipp:
Paradoxerweise behauptet das BayLDA in seiner lesenswerten Online-FAQ[6] exakt das Gegenteil. Dort heißt es nämlich:

„FRAGE: Dürfen Social PlugIns z. B. von Twitter, Facebook, Instagram auf der Website eingebunden werden?
ANTWORT: Ja. Allerdings muss vorher eine Einwilligung des Nutzers eingeholt und in der Datenschutzerklärung über den Einsatz informiert werden. Weitere Informationen: Heise 2-Klicklösung.“

Und hinsichtlich Google Analytics ist in der BayLDA-FAQ nachzulesen:

„FRAGE: Darf Google Analytics ohne Einwilligung des Nutzers auf der Website eingesetzt werden?
Antwort: Nein. Unabhängig davon, ob die IP-Adresse gekürzt wird oder nicht, muss eine Einwilligung eingeholt werden.“

Auf den ersten Blick hört sich dies so an, als ob die Einwilligung der Weisheit letzter Schluss sei. Dies ist auch theoretisch richtig, weil in der Theorie die Möglichkeit einer Einwilligung besteht. In der Praxis scheitert diese Variante jedoch an den fehlenden Informationen, die der Webseiten-Betreiber selbst hat.

Auch wenn die 2-Klick-Lösungen oder Cookie-Banner weitab von einer perfekten Lösung sind, empfehlen wir im Zweifel gleichwohl ihren Einsatz, da so der Webseiten-Betreiber dokumentiert, dass er alles ihm Mögliche getan hat.

bb. Berechtigte Interessen

Will sich ein Webseiten-Betreiber alternativ auf die berechtigten Interessen nach Art. 6 Abs. 1 f) DSGVO stützen, so ist es nach Ansicht des EuGH ebenso notwendig, dass er darüber informiert, in welchem Umfang der Tool-Anbieter die Daten verarbeitet.

Hier tritt exakt das gleiche Problem auf, das wir bereits von der Einwilligung her kennen: Da der Webseiten-Betreiber nicht genau weiß, was das von ihm eingesetzte Tool in letzter Konsequenz macht, kann er auch keine Abwägung der berechtigten Interessen vornehmen.

Somit ist ihm, jedenfalls nach Ansicht des BayLDA, daher auch ein Berufen auf die berechtigten Interessen nicht möglich.

Praxis-Tipp:
Paradoxerweise scheint das BayLDA hier zwischen einzelnen Tools zu differenzieren, so jedenfalls die aktuellen Ausführungen der lesenswerten Online-FAQ.[7] Ein Grund, warum die Behörde hier zwischen einzelnen Tools unterscheidet, ist in keiner Weise nachvollziehbar.
Danach soll z. B. die Einbindung externer Schriftarten (z. B. Google Fonts) unproblematisch erlaubt sein, obgleich auch hier personenbezogene Daten übertragen werden und somit hier eigentlich die identische Problemlage besteht.

c) Ergebnis

Aktuell können somit weder Social-Plug-ins noch externe Tracking-Tools rechtskonform in eine Webseite eingebunden werden. Und zwar sowohl aus formalen als auch aus inhaltlichen Gründen.

Jeder Webseiten-Betreiber sollte daher überprüfen, ob er zwingend auf ihren Einsatz angewiesen ist und ob er nicht auf rechtlich unproblematische Varianten (z. B. Matomo anstatt Google Analytics) ausweichen kann.¶