Dr. Martin Bahr

Warum alle Cookie-Banner rechtswidrig sind – und dennoch empfehlenswert

Auch wenn die zahlreichen Anbieter unterschiedlicher Content-Management-Tools etwas anderes behaupten: Alle aktuellen Cookie-Banner sind rechtswidrig, da sie sämtlich nicht mit der DSGVO vereinbar sind. Eine aktuelle Entscheidung der dänischen Datenschutzbehörde zeigt dies noch einmal sehr anschaulich. Der Artikel beleuchtet den aktuellen Rechtsstand und zeigt auf, warum es gleichwohl empfehlenswert sein kann, über ein Cookie-Banner nachzudenken.

A. Das unbekannte Wesen: das rechtskonforme Cookie-Banner

Es gibt im Online-Bereich ein bislang unbekanntes Wesen, das bis dato noch nie in der alltäglichen Praxis gesichtet wurde – nämlich das rechtskonforme Cookie-Banner.

Auch wenn die zahlreichen Anbieter unterschiedlicher Content-Management-Tools vollmundig etwas anderes versprechen: Keines dieser Banner-Werkzeuge ist mit den Regelungen der DSGVO in Einklang zu bringen. Dies hat einfach einen Grund: Nicht die Anbieter arbeiten falsch oder schlampig, sondern die gesetzlichen Anforderungen sind unerfüllbar. Es wird hier nämlich die sprichwörtliche Quadratur des Kreises gefordert.

1. Die Wurzel allen Übels: fehlende Umsetzung der E-Privacy-VO

Der Grund für diese missliche Lage ist relativ leicht ausgemacht. Die Wurzel allen Übels ist die fehlende Umsetzung der E-Privacy-Verordnung.

Ursprünglich sollte die neue E-Privacy-VO parallel mit der DSGVO im Jahr 2018 in Kraft treten. Dies ist aber bis heute nicht der Fall: Nach wie vor haben sich die EU-Länder nicht auf eine einheitliche Regelung verständigen können. Eine Lobbyschlacht nach der anderen wurde hier geschlagen. Zum überwiegenden Teil zu Recht, denn die bislang vorgestellten Entwürfe würden den Online-Bereich zu großen Teilen ins elektronische Mittelalter zurückkatapultieren. Die Umsetzung wurde verschoben und verschoben. Es ist nicht absehbar, ob überhaupt und wann hier etwas kommt.

Diese fehlende Umsetzung führte dazu, dass auf den Online-Bereich nun zwangsmäßig die Regelungen der DSGVO angewendet werden, um das bestehende Rechtsvakuum zu füllen. Und hier liegt auch die grundlegende Problematik: Es wird nun ein Gesetz angewendet, dass eigentlich für den Online-Bereich nicht gelten sollte. Die dadurch entstehenden Probleme sind also vorprogrammiert.

2. Regelungen der DSGVO

Für den Bereich des Online-Trackings bietet die DSGVO bekanntermaßen zwei Möglichkeiten an:

» Einwilligung
» berechtigte Interessen

a. Die Eier legende Wollmilchsau: die Einwilligung

Bei der Einwilligung gibt der User seine Zustimmung zu einer bestimmten Datenverarbeitung durch das Tracking-Unternehmen. Voraussetzung hierfür ist, dass der Nutzer zuvor ausreichend transparent und umfassend informiert wurde. Dies gilt für sämtliche Einwilligungen, sei es nun für den Offline- oder den Online-Bereich.

Das Unternehmen muss also darüber aufklären:

» An wen genau gehen die Daten des Users? Dabei müssen die Empfänger namentlich genannt werden.

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.

» Welche Daten genau werden übermittelt? Die Inhalte müssen einzeln benannt werden. Allgemein-Plattitüden wie „Ihre Marketing-Daten“ oder „alle relevante Daten“ sind nicht ausreichend.

Und hier zeigt sich auch, was die Einwilligung in der Online-Praxis wert ist: nämlich nichts. Anbieter aus dem E-Mail-Marketing schlagen sich seit mehr als 20 Jahren mit den unerfüllbaren Anforderungen der Rechtsprechung herum. Die dort aufgestellten Kriterien sind 1:1 übertragbar auf den Tracking-Bereich.

Wie soll ein Anbieter, der Retargeting-Tools (wie z. B. Criteo) auf seiner Webseite einsetzt, wirksam darüber informieren, an wen die User-Daten gehen? Die meisten Empfänger sind dem Anbieter namentlich nicht bekannt, sondern er weiß lediglich, dass die Informationen ins Retargeting-Netzwerk eingespielt werden.

Gleiches gilt für den Einsatz von Tools wie Google Analytics oder den Facebook-Button: Keiner dieser Tool-Dienstleister gibt verbindliche Erklärungen ab, was er so speichert und für welche Zwecke er die Informationen verwendet. Der Webseiten-Betreiber kann also bereits aufgrund dieser fehlenden Informationen keine Transparenz herstellen. Konsequenz ist, dass die eingeholte Einwilligung eben nicht wirksam ist.

Einwilligungen, die mittels eines Cookie-Banners eingeholt werden, sind also nichts wert.

b. Eine echte Alternative? Berechtigte Interessen

Aufgrund dieser Problematik stürzen sich viele Anbieter auf die andere DSGVO-Möglichkeit: die berechtigten Interessen.

Dabei handelt es sich um ein Instrument, das mit der DSGVO eingeführt wurde. Danach können die berechtigten Interessen einen ausreichenden Grund für die Datenübermittlung darstellen. Dabei muss der Anbieter seine Interessen (z. B. Ausspielung von Online-Werbung) mit den Interessen des getrackten Users abfragen.

Aktuell wird hierzu praktisch jede Rechtsmeinung vertreten: Die Front der Datenschützer vertritt den Standpunkt, dass die Datenanalyse für die eigene Webseite erlaubt ist. Webseitenübergreifendes Tracking (wie z. B. bei Google Analytics oder im klassischen Retargeting) hingegen soll ausnahmslos verboten sein.

Genau die gegenteilige Auffassung hat die Werbeindustrie: So funktioniere eben das Internet. Wenn man den Datenschützern folge, bedeute dies das Ende der Online-Werbewirtschaft, wie wir sie heute kennen. Es können dann nur noch allgemeine, nicht-kontextbezogene Werbeeinblendungen ausgespielt werden. Zumal der Rest von Europa ganz offensichtlich diesen restriktiven Standpunkt nicht vertrete.

c. Entscheidung der dänischen Datenschutzbehörde

Schaut man sich die bisherige Rechtsprechung zu dieser Problematik in den letzten Jahrzehnten an, so muss man kein Prophet sein, dass die Gerichte kaum ein solch intensives webseitenübergreifendes Tracking ohne engere Beschränkungen erlauben werden.

In genau diese Problematik stößt nun eine aktuelle Entscheidung der dänischen Datenschutzbehörde (Nachzulesen online unter *https://bit.ly/3cUKvE6*.).

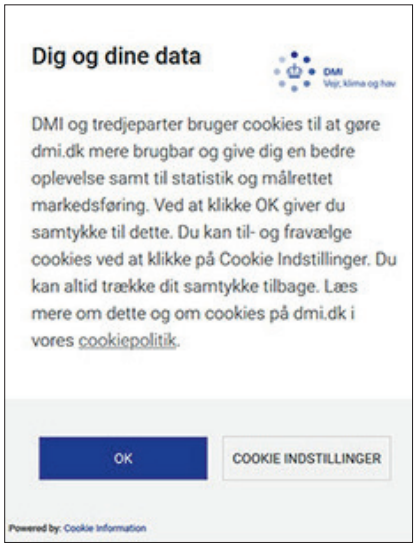
Es ging dabei um das Cookie-Banner auf der Webseite www.dmi.dk. Dieses war wie folgt ausgestaltet. In Form eines Pop-ups erschien der Text:

> „DMI und Dritte verwenden Cookies, um dmi.dk nützlicher zu machen und Ihnen eine bessere Erfahrung sowie Statistiken und gezieltes Marketing zu bieten. Wenn Sie auf OK klicken, stimmen Sie dem zu. Sie können Cookies auswählen und abwählen, indem Sie auf Cookie-Einstellungen klicken. Sie können Ihre Einwilligung jederzeit widerrufen. Lesen Sie mehr darüber und über Cookies auf dmi.dk in unserer Cookie-Richtlinie.“

Darunter gab es zwei Buttons:

> [OK] [Cookie Einstellungen]

Klickte der User auf „Cookie Einstellungen“, öffnete sich eine neue Seite, auf der die Cookies einzeln nach Rubriken unterteilt waren:



> „erforderlich
> funktional
> statisch
> Marketing
> nicht klassifiziert“

Die Webseite nutzte ein Tool des Dienstleisters Cookie Information A/S.

Das Design entsprach damit exakt der Ausgestaltung auch vieler prominenter Online-Webseiten in Deutschland und ist damit auf deutsche Verhältnisse nahtlos übertragbar.

Es ging bei der Auseinandersetzung nun um die Frage, ob durch das Pop-up-Fenster eine wirksame Einwilligung eingeholt wurde. Dies verneinte die dänische Datenschutzbehörde. Es fehle an der erforderlichen Transparenz, damit der Verbraucher eine wirksame Einwilligung abgeben könne:

> „Nach Ansicht der Datenaufsichtsbehörde ist die Zustimmung, die DMI durch die implementierte Lösung erhält, nicht ausreichend informiert.
> Insbesondere betont die Dateninspektion, dass es nicht genügend klare Informationen über die (gemeinsamen) für die Verarbeitung Verantwortlichen, einschließlich Google, in Zusammenarbeit mit denen gibt, mit denen personenbezogene Daten erhoben werden und an die personenbezogene Daten weitergegeben werden, und dass die betroffene Person nicht klar genug ist. Das wird gesammelt und an diese (gemeinsamen) Datenverantwortlichen, einschließlich Google, übertragen.
> In diesem Zusammenhang ist die Datenaufsichtsbehörde der Ansicht, dass im Hinblick auf die Einwilligung zur Verarbeitung personenbezogener Daten eine Einwilligungslösung oder -erklärung in leicht verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache erforderlich ist, aus der hervorgeht, welche für die Verarbeitung Verantwortlichen beteiligt sind. Beispielsweise werden persönliche Informationen weitergegeben. Im Folgenden ist zu beachten, dass die Identität des für die Verarbeitung Verantwortlichen angezeigt werden muss und nicht die vom Datenverantwortlichen verwendeten Websites, Spitznamen oder Produktnamen des Datenanbieters, da diese für die betroffene Person nicht leicht verständlich und leicht zugänglich sind.“

Ebenso kritisieren die Datenschützer die Darstellung der Buttons im Pop-up selbst:

> „Nach Ansicht der Dateninspektion erfüllt die derzeitige Struktur der Einwilligungslösung des DMI, bei der dem erstmaligen Besucher zwei Möglichkeiten in Bezug auf die Verarbeitung personenbezogener Daten angeboten werden; „OK“ und „Details anzeigen“, diese Transparenzanforderung nicht.
> In diesem Zusammenhang hat die Dateninspektion betont, dass es einem Besucher der Website nicht möglich ist, die Verarbeitung personenbezogener Daten während des ersten Besuchs bei dmi.dk abzulehnen. Der Besucher muss „Details anzeigen“ und dann „Zustimmung aktualisieren“ auswählen.
> Ein solcher „One-Click-Away“-Ansatz ist nach Ansicht der Datenaufsichtsbehörde nicht transparent, da er einen zusätzlichen Schritt erfordert, damit die betroffene Person die Zustimmung zur Verarbeitung personenbezogener Daten verweigert, und teilweise nicht, damit die betroffene Person daran scheitern kann, der Verarbeitung personenbezogener Daten durch Auswahl von „Details anzeigen“ zuzustimmen, ebenso wie der Wortlaut „Zustimmung aktualisieren“ Verwirrung stiften kann.
> In ähnlicher Weise entspricht es nach Ansicht der Datenaufsichtsbehörde nicht dem Grundsatz der Transparenz, dass die Möglichkeit, der Verarbeitung personenbezogener Daten in der DMI-Lösung nicht zuzustimmen, nicht den gleichen Kommunikationseffekt hat – das heißt, sie erscheint nicht so klar – wie die Möglichkeit, die Einwilligung zu erteilen, wodurch die betroffene Person indirekt dazu gedrängt wird, Einwilligung zur Verarbeitung personenbezogener Daten zu erteilen.“

Bedeutet im Klartext: Dieses und alle anderen Cookie-Banner im WWW sind rechtswidrig.

Es wird nur eine Frage der Zeit sein, bis auch Datenschutzbehörden und deutsche Gerichte diesen Standpunkt teilen.

2. Und was mache ich nun? Antwort: Nutzen Sie ein Cookie-Banner!

Viele Unternehmen fragen sich angesichts dieser katastrophalen Lage: Was soll ich denn machen?

Die Antwort ist simpel und einfach: Nutzen Sie ein Cookie-Banner!

Wie jetzt? Gerade eben hieß es doch, Cookie-Banner sind rechtswidrig. Wieso soll ich dann …?

Die erste Überlegung sollte sein: Benötige ich auf meiner Webseite überhaupt webseitenübergreifende Tracking-Technologien? In der alltäglichen Beratungspraxis zeigt sich nämlich immer wieder, dass viele Webseiten-Betreiber ein unnötiges Risiko eingehen. Wenn sie nämlich lediglich eine rein begrenzte Analyse ihrer eigenen Homepage durch entsprechende Tools

vornehmen (wie z. B. Matomo), dann können sie sich auf den oben erläuterten Grund der berechtigten Interessen stützen und müssen sich nicht auf die Unwägbarkeiten der Einwilligung verlassen.

Kommen Sie hingegen zu dem Ergebnis, dass Sie auf den Einsatz derartiger Tools nicht verzichten können: Nutzen Sie gleichwohl Cookie-Banner. Denn damit demonstrieren Sie, auch und insbesondere gegenüber den Aufsichtsbehörden, dass Sie sich redlich bemühen und Ihr Bestes gegeben haben. Im Rahmen eines etwaigen Bußgeldverfahrens wird es einen relevanten Unterschied machen, ob Sie einfach nichts getan haben oder ob Sie nicht vielmehr alles in Ihrer Macht Stehende getan haben, sich rechtskonform zu verhalten. Eines der Kriterien zur Bemessung etwaiger Strafen ist ausdrücklich das konkrete Verhalten des Unternehmens. Sie können hier also durch den Einsatz von Cookie-Bannern nur Pluspunkte sammeln.

Wichtig ist aber in jedem Fall: Der Einsatz von Cookie-Bannern führt, trotz aller vollmundigen Marketing-Versprechen, nicht dazu, dass Sie sich zu 100 % rechtskonform verhalten. Dessen müssen Sie sich bewusst sein. Wenn Sie bereit sind, dieses Risiko einzugehen, und zudem die zukünftige Rechtsprechung im Augenwinkel haben, steht einem Einsatz nichts (mehr) im Wege.

Zumal, traurigerweise, etliche europäische Datenschutzbehörden auf ihren Webseiten sich ebenso rechtswidrig verhalten und derartige Anwendungen einsetzen. Hier fragt man sich zu Recht: Welchen Sinn macht das alles, wenn selbst die Datenschutzbehörden in Europa keine rechtskonforme Ausgestaltung hinbekommen?