

von Rechtsanwalt **Jan Lennart Müller**

Dark Patterns bei Cookie-Consent Tools: Sind manipulative Tricks zulässig?

Beim Online-Shopping, auf der Suche nach Online-Zeitungsartikeln oder beim Recherchieren des Wetters der nächsten Tage - egal, welche Internetseite wir heute besuchen, auf allen werden wir von Cookie-Bannern begrüßt. Um die Einwilligung in die Verwendung von Cookies zu erlangen, wenden Webseiten-Betreiber manchmal den ein oder anderen kleinen Design-Trick an. Doch wie weit dürfen sie gehen? Welche Voraussetzungen bei der Erstellung von Cookie-Bannern eingehalten werden müssen und was es mit „Dark Patterns“ auf sich hat, lesen Sie im heutigen Beitrag.

I. Cookie-Einwilligungsbanner

Aufgrund der Datenschutz-Grundverordnung (DSGVO) sind Unternehmer verpflichtet, bei der Speicherung und dem Zugriff auf Informationen auf den Endgeräten (wie es z.B. bei der Verwendung von Cookies oder ähnlichen Technologien der Fall ist) Einwilligungen hierzu einzuholen. Dies ermöglicht es den Unternehmern beispielsweise, anhand der gesammelten Daten (z.B. Geschlecht, Interessen, besuchte Webseiten, etc.) personalisierte Werbung anzuzeigen.

Zu beachten ist, dass nicht allgemein jeder Einsatz von Cookies bzw. sämtliche Tracking-Maßnahmen einer gesonderten Einwilligung bedürfen, sodass eine solche Abfrage nicht immer nötig ist.

Da allerdings für einem Großteil der Cookies, die Unternehmer verwenden, eine Einwilligung erforderlich ist, fragen sie diese häufig mittels automatisch erscheinenden Bannern oder ähnlichen grafischen Elementen ab. Diese zeigen normalerweise eine Übersicht aller **einwilligungsbedürftigen Zugriffe auf das Endgerät** (gem. § 25 Abs. 1 TTDSG) sowie aller **Verarbeitungsvorgänge**, die gem. Art. 6 Abs. 1 lit. a) DSGVO gestützt werden, an.

1. Allgemeine Anforderungen an die Gestaltung

Zusätzlich zu den bestehenden gesetzlichen Anforderungen in der DSGVO veröffentlichte die Datenschutzaufsichtsbehörden im Dezember 2021 eine Orientierungshilfe für Anbieter von Telemedien, in der auch auf die Gestaltung von Einwilligungsbannern eingegangen wurde. Um eine wirksame Einwilligung zu erlangen, seien demnach einige Punkte bei der Gestaltung zu beachten.

Zunächst müssen alle Akteure und deren Funktion (Zugriff oder Datenverarbeitung) **ausreichend erklärt** werden. Die Vorgänge müssen dann über ein Auswahlmenü (aktiv) **aktiviert werden** können, es dürfe also **keine Voreinstellung** vorgenommen sein.

Obwohl es möglich sei, entsprechend des „Mehrebenenansatzes“ des EDSA Informationen über mehrere Stufen hinweg zu erteilen, müsse in dem automatisch erscheinenden Banner **auf erste Ebene jedenfalls folgende Informationen immer** angegeben werden:

- Information hinsichtlich des konkreten Zwecks der Verarbeitung
- Information ob individuelle Profile angelegt werden bzw. ob weitere Daten von anderen Webseiten gesammelt werden, um umfassende Nutzungsprofile anzulegen
- Information wenn Daten außerhalb des Europäischen Wirtschaftsraums verarbeitet werden
- Information hinsichtlich der Anzahl der Verantwortlichen, an die Daten offengelegt werden

a) Drittdienste:

Im Zusammenhang mit Drittdiensten, die beispielsweise für Zwecke des Nutzungstrackings oder der Erstellung von Nutzungsprofilen eingesetzt werden, sei es mindestens erforderlich, dieser Zwecke konkret zu erläutern. Ein einfacher Hinweis, dass Informationen an „Partner“ weitergegeben werden würden oder dass Drittdienste „die Informationen möglicherweise mit Weiteren Daten zusammenführen“, erfülle diese Anforderung nicht. Auch sei es nötig, die einzelnen Drittdienstleister zu benennen.

b) Laden der Skripte im Hintergrund:

Bis zur Erteilung der erforderlichen Einwilligung werden im Hintergrund zunächst keine Skripte geladen. Auch muss es den Webseiten-Besuchern auch vor Erteilung der Einwilligung **stets möglich sein**, auf das **Impressum sowie die Datenschutzerklärung zuzugreifen**. Erst ab Erteilung der Einwilligung dürfen beispielweise durch das Setzen eines Häkchens oder das Anklickens einer Schaltfläche darf auf Informationen zugegriffen bzw. dürfen diese gespeichert werden.

c) Ablehnfunktion auf erster Ebene:

Den Aufsichtsbehörden zufolge sei dies nicht generell erforderlich. Die Ablehnmöglichkeit müsse jedoch dann bereits auf erster Ebene angezeigt werden, **wenn Internet-Besucher mit dem Einwilligungsbanner interagieren müssen, um die Webseite weiter benutzen/vollständig sehen zu können** (meist der Fall). Sollte es ihnen jedoch möglich sein, die Webseite vollständig einzusehen, der Banner also keine Bereiche der Webseite versperrt, sei die Funktion entbehrlich. Hier müsse sichergestellt werden, dass sich der Banner auf allen Endgeräten gleich verhält.

Widerrufsmöglichkeit:

Da die Einwilligung stets widerruflich ist, müsse eine entsprechende Möglichkeit auf der Webseite angeboten werden. Diese müsse gem. Art. 7 Abs. 3 S. 4 DSGVO ebenso einfach ausgestaltet sein wie die Erteilung der Einwilligung.

2. Konkrete Gestaltung

Hinsichtlich der konkreten Gestaltung von Einwilligungsbannern betont die Orientierungshilfe der Aufsichtsbehörden, dass es **keinen allgemein geltenden Standard** gäbe. Es bestehe ein gewisser Spielraum hinsichtlich der Farbe, Größe oder Kontraste.

Bezwecken die Verantwortlichen durch eine konkrete Gestaltung des Einwilligungsbanner die Verhaltenssteuer der Webseiten-Besucher, wird dies als „**Nudging**“ bezeichnet. Dies sei zwar nicht generell unzulässig, finde seine Grenzen jedoch dort, wo die erforderlichen Voraussetzungen einer wirksamen Einwilligung nicht mehr gewahrt werden können (= „unzulässiges Nudging“). Dies sei insbesondere dann der Fall, wenn mehrere Gestaltungsmerkmale zusammenwirken würden.

a) Freiwilligkeit:

Eine wirksame Einwilligung erfordere einen freiwilligen Entschluss hierzu. Hieran könne es im Fall des Nudgings doch fehlen. Es sei nötig, dass eine tatsächliche Wahlmöglichkeit erkennbar sei und alle Möglichkeiten auch wählbar seien. Eine unterschiedliche Farbauswahl sei hier nicht per se problematisch.

An der Freiwilligkeit gezweifelt werden müsse allerdings dann, wenn alternative Optionen zur Einwilligung etwa ohne besondere Vorhebung in den Text eingebettet seien, sie außerhalb des Banners platziert werden oder aufgrund ihres Kontrasts/Schriftgröße nicht vollständig erkennbar seien. Diese seien dann nicht als gleichwertige Optionen zu bewerten. Alle Handlungsoptionen müssen auf einen Blick erkennbar sein, egal von welchem Endgerät zugegriffen werde.

b) Informierte Entscheidung:

Auch könne es fraglich sein, ob tatsächlich eine informierte Einwilligung vorliege, sollte ein Einwilligungsbanner zum Beispiel irreführende Informationen, bewusst verharmloste Sprache oder ein Überfluss an Informationen enthalten.

c) Ablehnoption:

Im Hinblick auf die genaueren Anforderungen der Ablehnoption sei es den Aufsichtsbehörden nach erforderlich, dass diese „**eindeutig erkennbar, leicht wahrnehmbar und unmissverständlich**“ sein. Die Option müsse insbesondere als **gleichwertige Option** dargestellt werden. Dies könne beispielsweise durch in Größe, Farbe, Kontrast und Schriftbild vergleichbare Buttons/Schaltflächen innerhalb des Einwilligungsbanners sichergestellt werden.

Es reiche nicht aus, wenn der Ablehnbutton erst nach Scrollen durch den ganzen Einwilligungstext erscheine, der Einwilligungsbanner allerdings von Anfang an klar sichtbar sei. Ebenfalls ungenügend sei es, sollte eine Schaltfläche „Einstellungen oder Ablehnen“ die Besucher lediglich auf eine weitere Ebene des Banners führen.

Auch wenn diese Punkte eine gute Orientierungshilfe bieten, müsse dennoch berücksichtigt werden,

dass es im Endeffekt von dem **Einzelfall** abhängt, ob noch von einer wirksamen Einwilligung gesprochen werden könne.

Eine weitere Orientierung bieten auch die Guidelines 3/2022 on Dark patterns in social media platform interfaces: how to recognise and avoid them (https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en). Diese seien überwiegend auch auf den Webseitenkontext übertragbar.

II. Dark Patterns

Trotz bestehender Vorgaben zeigt sich jedoch bei dem Vergleich von Cookie-Bannern auf verschiedenen Webseiten, dass viele Cookie-Banner es den Besuchern schwer machen, diese abzulehnen. Zwar ist es heutzutage nicht mehr nötig, alle Cookies einzeln abzuwählen. Dennoch werden kleine Tricks angewendet, die das Ablehnen der Cookies auf einem Großteil aller Seiten komplizierter gestalten als das Akzeptieren.

Solche Design-Tricks werden als „*Dark Patterns*“ bezeichnet, welche sich durch versteckte oder manipulative Gestaltungsmuster auszeichnen, die Webseiten-Besucher zu konkreten Handlungen (oder Nicht-Handlung, beispielweise das Unterlassen einer Kündigung, da der Kündigungsbutton nicht verortet werden kann) verleiten sollen. Dark Patterns können also nicht nur im Zusammenhang mit Cookies eingesetzt werden, sondern allgemein immer dann, wenn eine Handlung der Webseiten-Besucher (nicht) gewollt ist.

Hier gibt es viele verschiedene Arten von Dark Patterns, wie z.B:

1. Signalfarben

Häufig verwenden Webseiten **farblich verschiedene Buttons**, um Besucher so zu dem Akzeptieren ihrer Cookies zu bewegen. Hierbei werden „Cookies akzeptieren“-Buttons meist groß und in Signalfarben gestaltet, wohingegen andere Optionen in einem unauffälligeren Design, beispielweise weiß oder ausgegraut, designt sind.

Bist du einverstanden?

Wir benötigen deine Einwilligung, damit wir und unsere **Partner** technisch nicht notwendige Cookies und ähnliche Technologien einsetzen und so personenbezogene Daten (z. B. IP-Adresse) auf deinem Endgerät speichern bzw. abrufen können. Die Datenverarbeitung erfolgt für personalisierte Inhalte und Anzeigen (auf unseren und dritten Websites/Apps), Anzeigen- und Inhaltsmessungen sowie um Erkenntnisse über Zielgruppen und Produktentwicklungen zu gewinnen. Außerdem können wir so deine Nutzererfahrung innerhalb unserer Unternehmensgruppe (mobile.de GmbH) verbessern, dein Nutzungsverhalten analysieren sowie Segmente mit pseudonymisierten Nutzerdaten zusammenstellen und Dritten über unsere **Partner** einen Datenabgleich zur Personalisierung ihrer Werbung und die Möglichkeit anbieten, ähnliche Nutzer in ihrem eigenen Datenbestand zu identifizieren.

Möchtest du uns **keine Einwilligung** geben, klicke bitte **hier**. Einstellmöglichkeiten und mehr Infos zu den Zwecken und Partnern findest du unter "Datenschutzeinstellungen", für den jederzeit möglichen Widerruf der Einwilligung auch erreichbar über den Link im Footer/Menü.

Für die Auswahl sind Messung einfacher Anzeigen (von Kontextbezogene Werbung)

[Impressum](#) | [Datenschutzerklärung](#) | [Cookie-Erklärung](#)

Beispiel: kleinanzeigen.de, Hellgrün als Signalfarbe nur bei dem „Alle Akzeptieren“-Button, Option alle Cookies abzulehnen hier leicht übersehbar im Text versteckt

2. Komplizierte Gestaltung des Menüs

Viele Webseiten-Betreiber zählen darauf, dass Besucher die Alternative anklicken, die mit dem kleinsten Aufwand verbunden ist. Im Hinblick auf die „Alle Ablehnen“-Alternative kann deshalb bei vielen Seiten beobachtet werden, dass ein solcher Button, sollte er überhaupt als Button ausgestaltet sein, **häufig schwer zu finden** ist.

Während der „Alle Akzeptieren“-Button sofort auf der ersten Seite des Cookie-Banners gefunden und mit einem Klick ausgewählt werden kann, müssen Webseiten-Besucher sich oft erst mit **vielen Klicks durch komplizierte Menü-Punkte** navigieren, um letztendlich eine „Alle Ablehnen“-Option zu finden. Manchmal findet sich die Ablehn-Option auch nur in mitten des Cookie-Texts als unterstrichener Link und wird deshalb einfach übersehen (siehe obiges Beispiel: ebay-kleinanzeigen.de).

Die wohl einfachste Ausgestaltung, in der sowohl ein „Alle Akzeptieren“ als auch ein „Alle Ablehnen“-Button direkt auf der ersten Seite eines Cookie-Banners gleichberechtigt in gleicher Farbe und Größe angezeigt werden, lässt sich nur bei sehr wenigen Seiten finden.

Bsp: RTL.de, kompliziertes Menü, Signalfarbe bei „Alle Akzeptieren“-Button, keine gleichberechtigte Ablehnoption.

Bsp: gamesworld.de, kompliziertes Menü, aber gleichberechtigte „Alle Akzeptieren“- und „Alle Ablehnen“-Button, was nur sehr selten zu finden ist.

Datenschutz und Nutzungserlebnis auf RTL.de

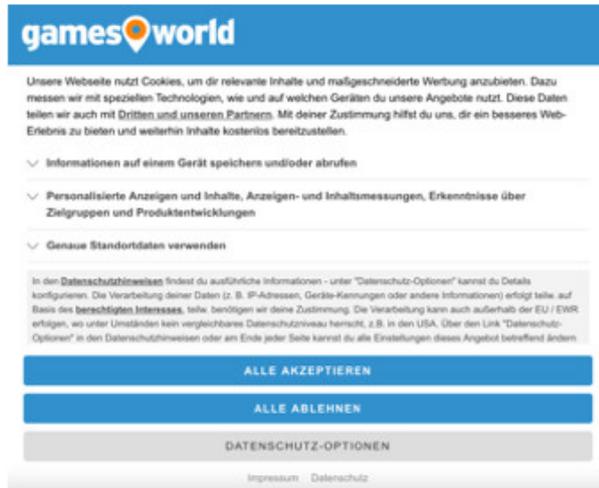
Wir und unsere [Partner](#) verarbeiten und übermitteln personenbezogene Daten (z.B. Identifier und Browserdaten) für die nachfolgend beschriebenen Zwecke. Hierzu werden Cookies und andere Technologien zur Speicherung und zum Zugriff auf Ihrem Gerät eingesetzt. Wir tun dies, um unser Angebot zu verbessern und zu finanzieren. In diesem Zusammenhang können Daten außerhalb des EWR verarbeitet werden und auch Nutzungsprofile gebildet und mit Daten von anderen Angeboten angereichert werden.

- Informationen auf einem Gerät speichern und/oder abrufen ▼
- Personalisierte Anzeigen und Inhalte, Anzeigen- und Inhaltsmessungen, Erkenntnisse über Zielgruppen und Produktentwicklungen ▼
- Fremdinhalte anzeigen (Soziale Netzwerke) ▼
- Angebotsübergreifende Verarbeitung von Daten durch Bertelsmann-Unternehmen für Analyse, Produktentwicklung, Messung, Werbung und Risikomanagement ▼
- Verwendung von netID ▼

Indem Sie „Alle Akzeptieren“ klicken, stimmen Sie (jederzeit widerruflich) diesen Datenverarbeitungen freiwillig zu. Dies umfasst auch Ihre Einwilligung zur Datenverarbeitung außerhalb des EWR (Art. 49 (1) (a) DSGVO, Drittlandtransfer), wo das hohe europäische Datenschutzniveau nicht besteht. Unter „Einstellungen oder ablehnen“ können Sie Ihre Angaben ändern oder Datenverarbeitungen ablehnen. Diese Einstellungen können Sie jederzeit im Privacy Center anpassen.

[Datenschutzerklärung](#) | [Impressum](#)

Beispiel: RTL.de, kompliziertes Menü, Signalfarbe bei „Alle Akzeptieren“-Button, keine gleichberechtigte Ablehnoption.



Beispiel: gamesworld.de, kompliziertes Menü, aber gleichberechtigte „Alle Akzeptieren“- und „Alle Ablehnen“-Button, was nur sehr selten zu finden ist.

Achtung bei der sog. "Click Fatigue (Klick-Ermüdung)":

Eine **wirksame** Einholung der Einwilligung des Seitenbesuchers setzt voraus, dass diese **freiwillig** erfolgt, d.h. eine echte und freie Wahl besteht und der Seitenbesucher die Möglichkeit hat, die Einwilligung zu verweigern oder zurückzuziehen, ohne dass ihm hieraus Nachteile entstehen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vertritt in ihrer [Orientierungshilfe](#) die Auffassung, dass das Merkmal der Freiwilligkeit beeinträchtigt ist, wenn die Verweigerung aller einwilligungsbedürftigen Zugriffe einen **messbaren Mehraufwand** bedeutet. Die DSK geht davon aus, dass ein solcher Mehraufwand vorliegt, wenn der Widerspruch **erst auf einer zweiten Bannerebene** und damit mit einer höheren Anzahl von Klicks möglich ist.

Der Mehraufwand besteht in der Regel auch nicht nur darin, dass der Seitenbesucher einmal mehr klicken muss als bei der Zustimmung. Vielmehr muss der Seitenbesucher zusätzlich die weiteren Informationen und Einstellungsmöglichkeiten, mit denen er auf einer zweiten Ebene der Einwilligungsdialoge konfrontiert wird, lesen, verstehen und aus den weiteren Auswahlmöglichkeiten die zutreffende auswählen.

Auch das [LG München I](#) hält die Ablehnungsmöglichkeit in einem Cookie-Consent Tool erst auf der zweiten Ebene für unzulässig.

3. Berechtigtes Interesse

Eine weitere unter den Webseiten-Betreibern beliebte Dark-Pattern-Variante ist die des „*berechtigten Interesses*“. Hierbei wird innerhalb der Banner eine Option angezeigt, mit der Cookies abgelehnt werden können.

Die von der Option umfassten Cookies werden hinter Schieberegler angezeigt, die den Anschein einer vollständigen Liste aller Cookies erweckt. Allerdings befinden sich unter einem Weiteren Menüpunkt „Berechtigtes Interesse“ weitere Auswahlmöglichkeiten an Cookies, die von der vorherigen Option nicht erfasst und somit auch nicht abgelehnt werden.

Problematisch hieran ist, dass das „berechtigte Interesse“ **sehr weit und sehr unterschiedlich definiert** werden kann und es Webseiten deshalb ermöglicht, zahlreiche weitere Cookies unter diesen Punkt zu fassen. Diese müssen in einem weiteren Schritt gesondert ausgewählt werden.

Selbst nach Abwahl aller Cookies muss hier in einem letzten Schritt auch darauf geachtet werden, dass diese Einstellungen **tatsächlich gespeichert werden**. Oftmals finden sich bei Cookie-Bannern auch am Ende einer solchen Auswahl neben den „Einstellungen speichern“-Buttons wiederum „Alles Akzeptieren“-Buttons, die oft wieder farblich hervorgehoben sind und mit einem Klick zum Akzeptieren aller Cookies führt.

Bsp: taz.de, gleichberechtigte Alternative, expliziter Hinweis, dass Verarbeitung der Daten teilweise auf der Grundlage des berechtigten Interesses erfolgt (Screenshot 1), bei Klick auf den „Selbst auswählen“-Button zeigt sich dann, dass weitere Cookies unter dem Punkt „Berechtigtes Interesse“ abgelehnt werden müssen (Screenshot 2)



Wir brauchen Ihre Zustimmung

Wir benötigen Ihre Zustimmung für den Datenaustausch mit unseren Werbepartner:innen, zur Verwendung von Cookies, um unser Webangebot zu analysieren, zu verbessern und zu finanzieren. Mit Ihrer Zustimmung helfen Sie uns dabei, taz.de für unsere User:innen zu verbessern. Widerrufen können Sie [hier](#) unter 6. Werbenetzwerke.

Informationen auf einem Gerät speichern und/oder abrufen

Personalisierte Anzeigen und Inhalte, Anzeigen- und Inhaltsmessungen, Erkenntnisse über Zielgruppen und Produktentwicklungen

externe Inhalte

Entscheiden Sie selbst, welche Cookies Sie zulassen wollen.

Selbst auswählen

Alles ablehnen

Alles akzeptieren

In den [Datenschutzhinweisen](#) finden Sie ausführliche Informationen und unter "Selbst auswählen" können Sie alle Details konfigurieren. Die Verarbeitung Ihrer Daten zu den oben genannten Zwecken erfolgt teilweise auf der Grundlage des berechtigten Interesses. Teilweise benötigen wir Ihre Zustimmung. Sie haben jederzeit die Möglichkeit, über den Privacy Manager in den Datenschutzhinweisen jegliche Einstellungen zu überarbeiten und jegliche Einwilligung zu widerrufen.

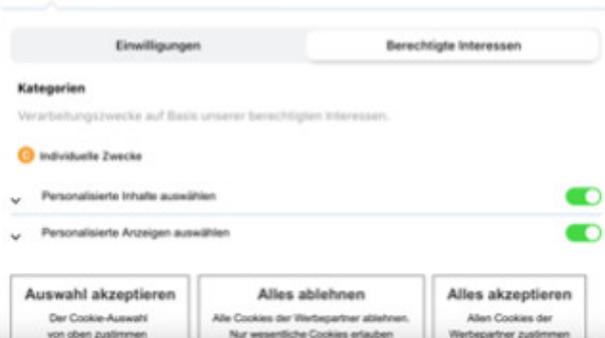
Beispiel: taz.de, gleichberechtigte Alternative, expliziter Hinweis, dass Verarbeitung der Daten teilweise auf der Grundlage des berechtigten Interesses erfolgt, bei Klick auf den „Selbst auswählen“-Button zeigt sich dann, dass weitere Cookies unter dem Punkt „Berechtigtes Interesse“ abgelehnt werden müssen (siehe hierzu nachstehenden Screenshot)

Ihre Einstellungen

Die Verarbeitung Ihrer Daten erfolgt teilweise auf der Grundlage des berechtigten Interesses, teilweise benötigen wir eine explizite Zustimmung. Mit einem Klick auf Kategorien können Sie unter Einwilligungen sehen, für welche Zwecke und welche Partner wir Ihre Einwilligung benötigen. Unter Berechtigte Interessen haben Sie die Möglichkeit, der Datenverarbeitung, die auf der Grundlage des berechtigten Interesses erfolgt, zu widersprechen.

Sie haben die Möglichkeit, die Datenverarbeitung nur für bestimmte Marketingpartner:innen zuzulassen. Unter Anbieter:innen können Sie Ihr Einverständnis individuell konfigurieren.

KATEGORIEN FUNKTIONEN ANBIETER



Einwilligungen Berechtigte Interessen

Kategorien
Verarbeitungszwecke auf Basis unserer berechtigten Interessen.

Individuelle Zwecke

Personalisierte Inhalte auswählen

Personalisierte Anzeigen auswählen

Auswahl akzeptieren
Der Cookie-Auswahl von oben zustimmen

Alles ablehnen
Alle Cookies der Werbepartner ablehnen.
Nur essentielle Cookies erlauben

Alles akzeptieren
Allen Cookies der Werbepartner zustimmen

4. PUR-Abos

Viele Online-Zeitschriften und andere Webseiten verfolgen eine andere Strategie: PUR Abos. Hierbei werden den Webseiten-Besuchern zwei Optionen geboten: Entweder sie akzeptieren die Cookies und können auf die Webseiteninhalte kostenlos zugreifen, oder sie **zahlen für Datenschutz** bzw. das PUR-Abo. Diese kosten zwischen 2,99 – 4,99 Euro im Monat.

Sie beinhalten jedoch meistens keinerlei Plus-Artikel oder andere Sonderleistungen, sondern bieten nur den normalen Umfang an Angeboten, die Nutzer, die den Trackingmaßnahmen von Anfang an zustimmen, auch erhalten. Die Abos sind für viele Webseiten-Besucher deshalb keine attraktive Option.

2018 entschied die österreichische Datenschutzbehörde jedoch, das das Angebot solcher PUR-Abos rechtmäßig sei.

Bsp: wetter.com, Alternative zwischen kostenlosem Zugriff auf Wetter-Dienste inkl. Werbung oder werbefreiem Zugriff für 2,99 Euro

Bsp: spiegel.de, auch hier Auswahl zwischen PUR-Abo oder Zugriff nur mit Werbung möglich

Akzeptieren & schließen

wetter.com

Mit Werbung weiterlesen ...

Besuche wetter.com wie gewohnt kostenlos und stimme der Verwendung von Cookies und anderen Technologien für Webanalysen und personalisierte Werbung (Tracking) zu.

Akzeptieren und weiter

Deine Einstellungen kannst du jederzeit in unseren Datenschutzhinweisen widerrufen. Mehr Informationen zu Werbung und Tracking findest du in unseren [Datenschutzhinweisen](#) und in den [Privatsphäre Einstellungen](#).

... oder mit contentpass

Nutze wetter.com und viele weitere Websites ganz ohne Werbefbanner, personalisiertes Tracking und Werbespots für nur 2,99€ / Monat.

Werbefrei für 2,99€ / Monat

Bereits contentpass-Mitglied? [Hier einloggen](#).

Wir nutzen ausschließlich Cookies und andere Technologien, die zur Bereitstellung unseres Angebotes unbedingt erforderlich sind. Details zum Abo findest du [hier](#) und in unseren [Datenschutzhinweisen \(contentpass-Abo\)](#).

Wir und unsere **Partner** verarbeiten personenbezogene Daten (wie z.B. IP- und Browserinformationen) für folgende Zwecke:

Informationen auf diesem Gerät speichern und/oder abrufen

[Impressum](#) | [Datenschutz](#)

Beispiel: wetter.com, Alternative zwischen kostenlosem Zugriff auf Wetter-Dienste inkl. Werbung oder werbefreiem Zugriff für 2,99 Euro

Herzlich willkommen!

Weiter mit Werbung lesen

Besuchen Sie SPIEGEL.de wie gewohnt mit Werbung und üblichem Tracking. (Zustimmung ist jederzeit widerrufbar.)

Akzeptieren und weiter >

Details zu Werbe- und Analytik-Trackern sowie zum jederzeit möglichen Widerruf finden Sie in unserer [Datenschutzerklärung](#) oder im [Privacy Center](#) am Ende jeder Seite.

Werbefrei lesen

Keine Weitergabe Ihrer Daten an Werbetreibende. Nutzen Sie uns kostengünstig ganz ohne Werbetacking und praktisch werbefrei.

Jetzt Details ansehen >

«Werbefrei lesen» bereits gebucht? [Hier ansehen](#).

Tracking: Zur Verbesserung und Finanzierung unseres Webangebots arbeiten wir mit Drittanbietern zusammen. Diese **Drittanbieter** und wir erheben und verarbeiten personenbezogene Daten auf unseren Plattformen. Mit auf Ihrem Gerät gespeicherten Cookies, persönlichen Identifikatoren wie bspw. Geräte-Kennungen oder IP-Adressen sowie basierend auf Ihrem individuellen Nutzungsverhalten können wir und diese Drittanbieter ...

- ... Informationen auf einem Gerät speichern und/oder abrufen: Für die Ihnen angezeigten Verarbeitungszwecke können Cookies, Geräte-Kennungen oder andere Informationen auf Ihrem Gerät gespeichert oder abgerufen werden.
- ... Personalisierte Anzeigen und Inhalte, Anzeigen- und Inhaltsmessungen, Erkenntnisse über Zielgruppen und Produktentwicklungen auspielen: Anzeigen und Inhalte können basierend auf einem Profil personalisiert werden. Es können mehr Daten hinzugefügt werden, um Anzeigen und Inhalte besser zu personalisieren. Die Performance von Anzeigen und Inhalten kann gemessen werden. Erkenntnisse über Zielgruppen, die die Anzeigen und Inhalte betrachtet haben, können abgeleitet werden. Daten können verwendet werden, um Benutzerfreundlichkeit, Systeme und Software aufzubauen oder zu verbessern.

Beispiel: spiegel.de, auch hier Auswahl zwischen PUR-Abo oder Zugriff nur mit Werbung möglich

III. Konsequenzen

Aufgrund der Verwendung der diversen Dark Patterns kann davon ausgegangen werden, dass die Cookie-Banner vieler Webseiten nicht mit der DSGVO im Einklang stehen, insbesondere gegen die **Grundsätze der Fairness, Transparenz, Information und Freiwilligkeit verstoßen**. Trotz der Orientierungshilfe vom Dezember 2021 sowie der daraufhin erlassenen Richtlinie zu Dark Patterns bei Sozialen Medien vom Frühjahr 2022 werden Dark Patterns immer noch häufig auf Webseiten gefunden. Die Aufsichtsbehörden erreichen deshalb regelmäßig Beschwerden wegen unrechtmäßiger Cookie-Banner.

IV. Aktuelle Entwicklungen - Warum sind Dark Patterns so weit verbreitet, wenn sie doch gegen die DSGVO verstoßen?

Wenn Dark Patterns bei Cookie-Bannern gegen das Gesetz verstoßen, könnte man sich fragen, warum sie dennoch so weit verbreitet sind. Manch Ansicht zufolge sei dies Schuld der Datenschutzbehörden, die die DSGVO mit ihrer Einführung im Jahr 2018 nicht streng **genug durchsetzten**.

Obwohl die Datenschutzbehörde in Belgien die gängige Cookie-Banner-Praxis in 2022 **für rechtswidrig erklärte**, sei noch nicht entsprechend strengen Strafen reagiert worden. Auch bleibe die Effektivität des neuen **Digital Service Act der EU** zur Bekämpfung der rechtswidrigen Cookie-Banner fraglich.

In Deutschland versucht auch das Bundesministerium Für Digitales und Verkehr (BMDV) gegen die Cookie-Banner vorzugehen. Insbesondere der **Entwurf zu einer Einwilligungsverwaltungsverordnung** versuche Webseiten-Besucher durch eine zentrale Voreinstellung und Verwaltung von Einwilligungen von vielen Einzelentscheidungen entlasten, beispielsweise durch ein Browser-Plugin. Wie dies genau umgesetzt werden soll, bleibt jedoch noch abzuwarten.

Eine weitere interessante Entwicklung hinsichtlich Cookies lässt sich bei den Unternehmen Apple und Google finden. Die beiden Unternehmen arbeiten seit ein paar Jahren daran, keine Third-Party-Cookies mehr in ihren Betriebssystemen zuzulassen. Obwohl dies primär ihrem Ziel dient, sich selbst eine Monopolstellung im Hinblick auf das Geschäft mit dem Online-Tracking zu verschaffen, hätte dies für Benutzer gleichzeitig den Vorteil, dass ihre Daten vor Dritten geschützt werden.

V. Fazit

Ein Blick auf die verschiedenen Webseiten im Internet zeigt, dass viele Unternehmer es den Webseiten-Besucher unnötig schwer machen, ihre Cookies abzulehnen, um an möglichst viele Einwilligungen zu gelangen. Mittels verschiedenster Methoden wie unauffälliger Links, Signalfarben oder komplizierter Gestaltung der Cookie-Banner erhoffen sie sich, möglichst viele Daten zu sammeln und diese weitergeben zu können.

Sie möchten mehr zum Thema "Dark Patterns" erfahren?

Für weitere Informationen empfehlen wir Ihnen unseren Beitrag [„10 Dark Patterns im Online-Handel-erkennen und vermeiden!“](#)

Autor:

RA Jan Lennart Müller

Rechtsanwalt