iubenda

iubenda.com

Die Zukunft von Cookie-Einwilligungen in Europa: Darauf sollten Vermarkter vorbereitet sein

Ihr praktischer Leitfaden zu Cookie-Einwilligungen in Europa für eine gesetzeskonforme Marketing-Strategie, die Ihr Wachstum vorantreibt.

Certified CMP Partner

Das Wichtigste auf einen Blick

Warum sind Cookies für Vermarkter so wichtig?

Weil sie sich direkt auf Ihre Marketing-Performance auswirken können. Jedes Mal, wenn ein Besucher Cookies ablehnt oder Ihr Banner ignoriert, entgehen Ihnen nicht nur wichtige Datenpunkte, sondern auch Conversion-Attributionen und Retargeting-Chancen.

Ihr Setup für Einwilligungen ist viel mehr als eine gesetzliche Formalität. Sie ist ein Teil Ihrer Marketing-Infrastruktur. Und wie gut Ihr Setup funktioniert, wirkt sich direkt auf die Qualität und Menge der Ihnen zur Verfügung stehenden Daten aus.

Warum sind Cookie-Einwilligungen in Europa gerade im Wandel?

Das aktuelle System sorgt auf beiden Seiten für ordentlich Reibung. Ihre Nutzer sehen jeden Tag Hunderte von Bannern, nehmen sie kaum zur Kenntnis und klicken sich müde durch. Für Unternehmen wird es wiederum immer schwieriger, ihre Setups auf die behördlichen Vorgaben auszurichten.

Die EU hat dieses Problem erkannt und arbeitet an einfacheren Lösungen, ohne Kompromisse in Sachen Datenschutz einzugehen. In Zukunft sollen deshalb seltener und eindeutigere Interaktionen zur Einwilligung erfolgen. In die Nutzung von Werbe- und Tracking-Cookies muss weiterhin aktiv und ausdrücklich eingewilligt werden (Opt-in). Das Verfahren ändert sich, das Prinzip bleibt jedoch das gleiche.

Hat sich denn schon irgendetwas geändert?

Nein. Anfang 2026 hat die EU einen Gesetzesentwurf veröffentlicht, aber noch kein gültiges Gesetz. Die aktuellen DSGVO- und ePrivacy-Vorgaben gelten also auch weiterhin. Das heißt, Sie müssen Ihr Setup nicht sofort von Grund auf neu gestalten. Es ist jedoch klar, wohin der Weg führt. Und Teams, die sich jetzt schon vorbereiten, haben einen klaren Vorteil, wenn die Änderung dann tatsächlich umgesetzt wird.

Worauf sollten sich Vermarkter ab 2026 konzentrieren?

- Behandeln Sie Ihr Einwilligungs-Setup als Teil Ihrer Marketing-Infrastruktur, nicht nur als gesetzliche Vorgabe, die Sie abhaken müssen. Sehen Sie Datenschutzpraktiken als wichtige Treiber für Markenvertrauen und Kundenbindung an.
- Nutzen Sie datenschutzsensible Ansätze Ihrer Consent Manager Platform (CMP): Google Consent Mode stellt mehr als 70 % der Conversion-Klickpfade wieder her, die durch das Ablehnen von Cookies verlorengegangen sind. Die Integration des IAB Transparency and Consent Framework ist und bleibt für Vermarkter enorm wichtig.
- Erstellen Sie eine Strategie für First Party-Daten, also Daten, in deren Nutzung Ihre eigene Zielgruppe eingewilligt hat. Diese sind die verlässlichste Datenquelle für bessere Personalisierung.
- Verfolgen Sie Ihre Einwilligungsrate als Leistungskennzahl und testen und optimieren Sie Ihre Banner, um mehr Opt-ins zu erzielen.

Was ist eine Einwilligungsrate und warum ist sie so wichtig?

Eine Einwilligungsrate beschreibt den Prozentsatz Ihrer Besucher, der aktiv Cookies akzeptiert (Opt-in). Sehen Sie es als eine Art Einstiegspunkt für all Ihre Marketing-Daten an: Je mehr Nutzer einwilligen, desto mehr Daten stehen Ihnen für Analysen und Werbeplattformen zur Verfügung. Mehr Daten bedeuten gezielteres Targeting, genauere Attributionen und bessere Ergebnisse. Die Einwilligungsrate ist eine Wachstumskennzahl. Deshalb sollten Sie sie auch als solche behandeln.

Inhalt

Back to Basics: So funktionieren Cookie-Einwilligungen 2026

Bevor wir einen Blick auf die bevorstehenden Änderungen werfen, wollen wir uns noch einmal den Basics widmen: was Cookies sind, warum Einwilligungen so wichtig sind und wie das System aktuell aufgebaut ist. Egal, ob Sie gerade Ihre ersten Schritte machen oder eine kurze Auffrischung brauchen, dieser Abschnitt beantwortet alle grundlegenden Fragen.

Was sind Cookies?

Cookies sind kleines Textdateien, die Websites auf Ihrem Gerät speichern, sobald Sie sie aufrufen. Sie erinnern sich an Dinge wie Ihre Login-Daten, bevorzugte Sprachen oder den Inhalt Ihres Warenkorbs. Einige Cookies werden direkt von der Website installiert, die Sie besuchen. Andere stammen von externen Diensten, die auf der jeweiligen Seite eingebettet sind, darunter Werbenetzwerke, Social Media-Plugins oder Analytik-Anbieter.

Diese Unterscheidung ist wichtig, weil die Datenschutzbestimmungen der EU diese beiden Cookie-Arten unterschiedlich behandeln.

First-Party-Cookies	Drittanbieter-Cookies
Stammen von der Website, die Sie gerade besuchen	Stammen von externen Diensten (Werbenetzwerke, Social Media-Plattformen, Analytik-Anbieter)
Sorgen für einen reibungslosen Ablauf wichtiger Funktionen: Login, Einstellungen, Warenkorb	Ermöglichen Werbeanzeigen, seitenübergreifendes Tracking und Social Media-Funktionen
Allgemein geringeres Datenschutzrisiko	Erfordern meistens eine Einwilligung gemäß EU-Gesetzgebung

Für Ihre alltäglichen Marketing-Tools sind **Drittpartei-Cookies** unverzichtbar: Retargeting-Pixel, Conversion-Tracking, Zielgruppensegmentierung und personalisierte Werbeanzeigen. Sie erfordern jedoch auch am häufigsten eine Einwilligung.

Warum ist für die Installation von Cookies eine Einwilligung erforderlich?

Stellen Sie sich Cookies als einen Haftnotizzettel vor, den eine Website auf Ihrem Gerät hinterlässt. Einige dieser Notizen sind wirklich hilfreich, zum Beispiel wenn sich Ihr Gerät dadurch merkt, dass Sie bereits eingeloggt sind. Andere wiederum halten fest, wie Sie im Internet navigieren, was Sie kaufen, wonach Sie suchen und wer Sie sind.

Laut Gesetz müssen Websites deshalb vor dem Einsatz solcher Cookies um Ihre Erlaubnis bitten, **denn Besucher sollten stets die Kontrolle über ihre Daten und das Recht haben, der Erfassung und Verwendung ihrer Daten zu widersprechen.**

Aktuelle Regeln rund um die Nutzung von Cookies

Es gibt zwei EU-Gesetze, die gemeinsam dafür sorgen, dass die Rechte der Nutzer bei der Verwendung von Cookies geschützt werden:

- **Die ePrivacy-Verordnung** (oft auch als „Cookie-Gesetz“ bezeichnet) verlangt, dass Websites ihre Nutzer darüber informieren, wie sie Daten auf den Geräten speichern und nutzen, und vor der Nutzung eine Einwilligung einholen.

- **Die Datenschutz-Grundverordnung (DSGVO)** legt strenge Regeln für die Verarbeitung personenbezogener Daten fest. Diese Regeln gelten auch für Daten, die durch Cookies erfasst wurden.

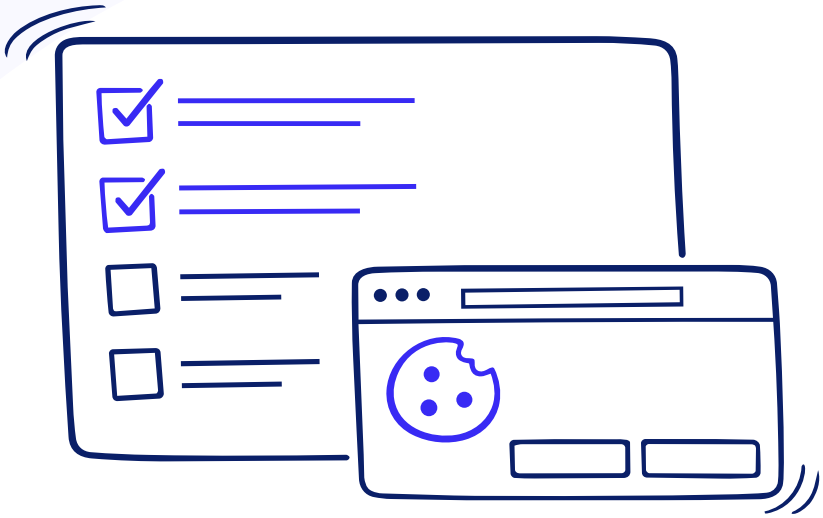
Sie bilden zusammen ein zentrales Prinzip: Bevor ein optionaler Cookie auf dem Gerät eines Nutzers ausgeführt wird, muss dieser darüber informiert werden und seine explizite Einwilligung geben.

Die einzigen Ausnahmen?

- Technisch notwendige Cookies: Diese werden für grundlegende Website-Funktionen (zum Beispiel dafür, dass ein Nutzer eingeloggt bleibt) oder das Übermitteln von Mitteilungen benötigt.

- In einigen EU-Mitgliedstaaten erfordern bestimmte Analyse-Cookies keine Einwilligung, solange einige strenge Voraussetzungen erfüllt sind (z. B. begrenzte Geltungsbereiche, Anonymisierung, kein seitenübergreifendes Tracking).

Alle sonstigen Cookies **erfordern zuerst ein klares „Ja“.**



Wie genau sieht also eine „informierte, ausdrückliche Einwilligung“ in der Praxis aus?

Das sind die wichtigsten Anforderungen für Europa. Wenn Ihre Website Nutzer in der EU anspricht und optionale Cookies verwendet, ist es sehr wahrscheinlich, dass Sie alle erfüllen müssen:

Cookies vor der Einwilligung blockieren

Optionale Cookie-Skripts dürfen nicht ausgeführt werden, bis Ihre Nutzer aktiv einwilligen. Wichtig: Vorausgewählte Kontrollkästchen oder implizierte Einwilligungen sind nicht erlaubt.

Nutzer vor der Einwilligung informieren

Erklären Sie Ihren Nutzern, welche Cookies Sie verwenden, welche Funktion sie haben und welche Drittanbieter Sie nutzen. Verlinken Sie auf die einzelnen Datenschutzerklärungen der Drittanbieter.

Nutzern die Wahl lassen

Die Option zum Ablehnen muss genau so deutlich sichtbar und leicht zugänglich sein wie die Option zum Annehmen.

Optionen für individuelle Einstellungen bereitstellen

Nutzer müssen wählen können, welche Cookie-Kategorien sie akzeptieren (z. B. Analysecookies: Ja, Werbe-Cookies: Nein).

Widerruf jederzeit ermöglichen

Ihre Nutzer müssen Ihre Einwilligung ändern oder widerrufen können. In der Regel erfolgt der Widerruf über ein Datenschutz-Widget.

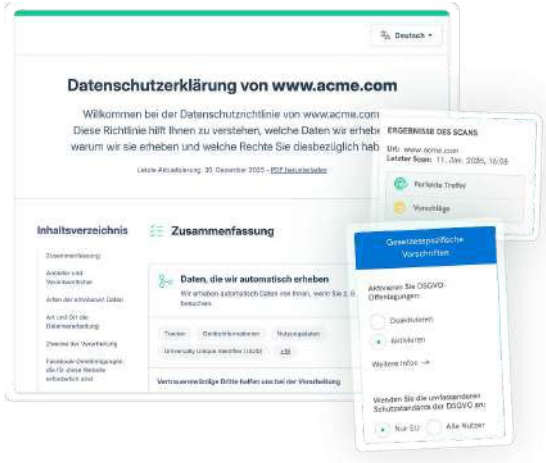
Einwilligungsnachweis dokumentieren

Erfassen Sie, wann und wie Ihre einzelnen Nutzer ihre Einwilligung erteilt haben, damit Sie bei Bedarf **nachweisen können, dass Sie Ihre Pflicht erfüllt haben**.

Wenn Sie Drittanbieter-Cookies verwenden, sind sowohl Sie als auch der Drittanbieter dafür verantwortlich, Ihre Nutzer angemessen zu informieren. Die einfachste Lösung dafür ist eine Datenschutzerklärung und Cookie-Richtlinie.

In Ihrer Cookie-Richtlinie müssen alle Dienste mit Namen und Zweck aufgeführt sein. Achtung: Dieses Level an Transparenz ist auf keinen Fall optional, sondern essenziell, um die für Europa geltenden Anforderungen zu erfüllen.

Aber Rechtsdokumente zu erstellen und auf dem neuesten Stand zu halten, kann nervenaufreibend sein.

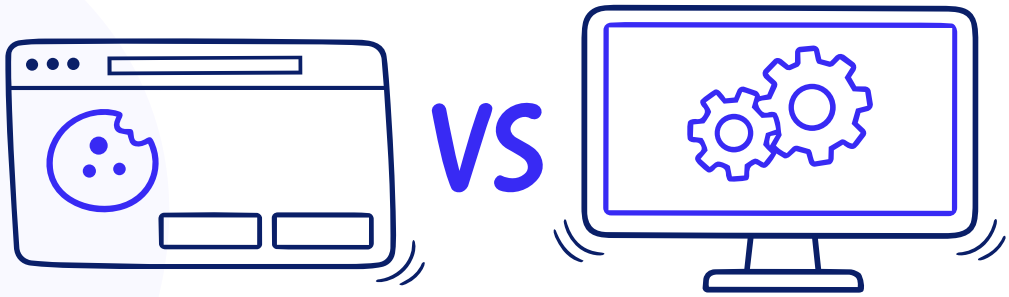


Werfen Sie einen Blick auf unseren Generator für Datenschutz- und Cookie-Richtlinien

Die Bedeutung von Cookie-Bannern und CMPs

Die meisten Leute denken bei dem Begriff „Cookie-Einwilligung“ an das Banner, das erscheint, wenn man eine Website besucht. Aber das Banner ist nur ein Teil des Puzzles. Dahinter steckt in der Regel eine Consent Management Platform (kurz CMP), die für die technische Durchsetzung der Nutzerpräferenzen zuständig ist.

Diese beiden Elemente arbeiten zusammen, haben aber unterschiedliche Zuständigkeitsbereiche:



Cookie-Banner

Das Banner ist eines der ersten Elemente auf Ihrer Website, die Ihre Besucher sehen. Dabei handelt es sich um den Hinweis, der beim ersten Besuch erscheint. Es informiert Ihre Nutzer über Cookies und gibt ihnen die Möglichkeit, sie zu akzeptieren, abzulehnen oder ihre Einstellungen anzupassen. Ihr Banner ist also nicht nur eine reine Formalität, sondern die Eingangstür zu Ihrem Einwilligungs-Setup.

Consent Management Platform (CMP)

Die CMP ist das System hinter Ihrem Banner. Sie kümmert sich um alle technischen und rechtlichen Aufgaben und:

- **Erfasst und speichert Einwilligungspräferenzen**
- **Blockiert oder aktiviert Cookie-Skripts je nach Nutzerpräferenzen**
- **Dokumentiert Einwilligungsnachweise für Ihre Unterlagen**
- **Verbindet sich mit Ihren Werbeplattformen, Ihren Analyse-Tools und Ihrem Marketing-Stack**
- **Unterstützt Rahmenwerke wie den IAB Transparency and Consent Framework (TCF) und den Google Consent Mode**

Ihr Banner gibt Ihren Nutzern die Wahl. Die CMP sorgt dafür, dass diese auch umgesetzt wird.

Ohne ein vernetztes System ist Ihr Banner nur ein dekoratives Pop-up ohne echte Funktion. Denn egal wie Ihre Nutzer sich entscheiden, Skripte würden trotzdem ausgeführt werden – und das ist alles andere als gesetzeskonform.

Warum Cookie-Einwilligungen für Ihr Marketing so wichtig sind

„Bevor ich zu iubenda gestoßen bin, bin ich davon ausgegangen, dass Cookies und Datenschutz nichts mit Marketing zu tun haben. Das Rechtsteam legt den rechtlichen Rahmen fest und die Marketingabteilung sorgt dafür, dass dieser Rahmen nicht gesprengt wird. Da lag ich falsch. Wenn Sie im Marketingbereich arbeiten und nicht genau wissen, wie Sie Daten erfassen und verwenden, lohnt es sich, einmal genauer hinzusehen."

Andreea Mandeal,
CMO bei iubenda

Cookie-Einwilligungen wirken sich direkt auf die Marketing-Performance aus.

Jedes Mal, wenn ein Nutzer Cookies ablehnt oder Ihr Banner ignoriert, **entgeht Ihnen die Chance auf wertvolle Daten, Conversion-Attributionen und Retargeting.** Auf Ihre gesamte Zielgruppe gesehen, machen sich diese Auswirkungen schnell bemerkbar.

In diesen Bereichen wird Ihre Marketing-Performance am meisten beeinträchtigt:

Datenqualität

Wenn Ihre Nutzer nicht einwilligen, können Sie schlechter nachvollziehen, wie sie mit Ihrer Website interagieren. Ihre Analysen können nur ein unvollständiges Bild wiedergeben und Bidding-Algorithmen nur einen Teil der Daten nutzen.

Attribution und Conversion-Tracking

Keine Einwilligung bedeutet kein Conversion-Tracking, kein Retargeting und keine Personalisierung von Werbeanzeigen für Ihre Nutzer. Ihre Attributionsmodelle werden unzuverlässiger, wodurch es schwerer wird zu verstehen, was genau für Ergebnisse sorgt – und was nicht.

Kampagnen-Optimierung

Werbeplattformen setzen auf Conversion-Daten, um die Anzeigenschaltung zu optimieren. Weniger Daten bedeutet weniger zielgerichtete Optimierung, höhere Kosten bei der Akquisition und weniger Gewinn pro Anzeige.

Markenvertrauen

Wie Sie mit Einwilligungen umgehen, hat direkte Auswirkungen darauf, wie Nutzer Ihre Marke wahrnehmen. Ein verwirrendes oder gar aggressives Banner kann schnell dazu führen, dass potenzielle Kunden das Vertrauen in Ihre Marke verlieren. Ein klares, respektvolles Banner bewirkt, dass das Vertrauen gestärkt wird. Laut der **Cisco Consumer Privacy Umfrage aus dem Jahr 2024** geben 75 % der Verbraucher an, dass sie nicht bei Unternehmen einkaufen, denen sie ihre Daten nicht anvertrauen möchten. Es steht also sehr viel mehr auf dem Spiel als nur Kennzahlen.

Das Ende einer Ära? Cookie-Einwilligungen am Scheidepunkt

Cookie-Einwilligungen funktionieren in Europa seit Jahren gleich: Banner anzeigen, um Einwilligung bitten, Cookies bis zur Einwilligung blockieren. Dieses System wurde entwickelt, um einen angemessenen Datenschutz zu gewährleisten. Aber es führte genauso zu ordentlich Reibung, weshalb sich die Europäische Union nun der Aufgabe angenommen hat, die Situation zu verbessern.

Warum ist es Zeit für eine Veränderung?

Das aktuelle Einwilligungsmodell übt auf beiden Seiten des Bildschirms Druck aus. Nutzer sind der vielen Banner überdrüssig. Unternehmen verlieren durch die Komplexität den Überblick. Eine echte Lose-Lose-Situation.

Auf Seiten der Nutzer

Nutzer gehen immer bewusster mit ihren Daten um - und sie machen sich Sorgen... Laut **Eurostat-Daten aus dem Jahr 2025,** haben 76,9 % der Internetnutzer in der EU aktiv Maßnahmen ergriffen, um ihre personenbezogenen Daten online zu schützen. Im Jahr 2023 waren das noch 73,2 %. Datenschutz wird immer wichtiger und Internetnutzer werden immer aktiver, um ihre Daten zu schützen.

...haben aber Einwilligungen genauso satt. Da werden die meisten sicherlich zustimmen. Auf fast jeder Seite sehen wir ein Cookie-Banner. Wir lesen sie nicht, klicken auf „Annehmen“, damit sie verschwinden, oder lehnen aus Frustration direkt alles ab. So oder so: Das ist keine echte informierte Einwilligung und ständiges erneutes Abfragen ist lästig.

Schlechte Banner-Designs machen es noch schlimmer. Einige Websites können gar nicht richtig aufgerufen werden, weil Ihr Banner langsam oder aufdringlich ist. In dem Fall verlassen Nutzer lieber die Website und wechseln zur nächsten. Viele Banner nutzen noch immer manipulative Designs: größere oder hellere Annahme-Buttons, fehlende Optionen zum Ablehnen, vorausgewählte Kontrollkästchen, die eine Einwilligung voraussetzen.

Auf Seiten der Unternehmen

Die rechtliche und technische Seite ist ein echtes Problem. Es gibt viele rechtliche Anforderungen. Und von Land zu Land oder je nach Gesetzgebung können sie unterschiedlich ausfallen.

Auf dem Laufenden bleiben -- leichter gesagt als getan. Ein Compliance-Setup ist nichts, das man einmal aufsetzt und dann vergessen kann. Mit neuen Vorschriften ändern sich Rechte und Pflichten immer wieder. Unternehmen haben alle Hände voll zu tun mit Updates, Anpassungen an ihren Setups und sich anhäufenden Kosten. Für kleinere Teams kann sich das besonders überwältigend anfühlen.

Negative Auswirkungen auf Umsatz und höhere Risiken. Die Kombination von mangelhaften Einwilligungsabläufen, unvollständigen Daten und steigenden Compliance-Kosten wirkt sich auf die Performance aus. Und wenn Ihr Einwilligungs-Setup nicht alle Anforderungen erfüllt, kommt die Gefahr behördlicher Konsequenzen hinzu.

Das Einwilligungssystem für Cookies in Europa sollte Nutzern ursprünglich die Kontrolle zurückgeben. Jetzt sind sie müde und frustriert.
Im **Explanatory Memorandum** der Europäischen Kommission hat diese anerkannt, dass „die Verbreitung von Cookie-Bannern und die diesbezügliche ‘Einwilligungsmüdigkeit’ eine längst überfällige regulatorische Lösung“ erfordert.

So reagiert die EU

Der neue Digital Omnibus-Vorschlag

Im November 2025 hat **die Europäische Kommission ihren Digital Omnibus-Gesetzesentwurf veröffentlicht.**

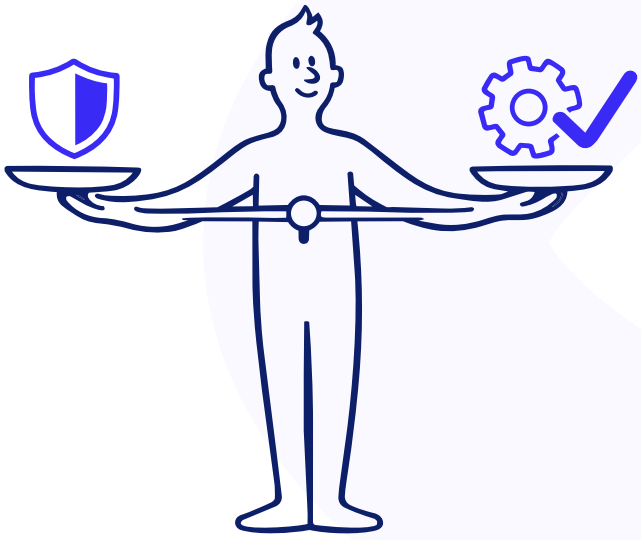
Er ist Teil eines umfassenden Pakets zur Vereinfachung und Modernisierung der digitalen Regeln innerhalb der EU, ohne die **fundamentalen Datenschutzrechte zu beschneiden, die die europäische Gesetzgebung im Laufe der letzten zwei Jahrzehnte aufgebaut hat**.

Damit erklärt die EU den Wunsch, die beobachteten Herausforderungen anzugehen und ein Gleichgewicht zu finden, das für weniger Reibung auf Seiten der Nutzer und weniger Komplexität und Kosten auf Seiten der Unternehmen sorgt.

- Vereinfachte Interaktion zwischen ePrivacy-Vorschriften und der DSGVO
- Weniger Einwilligungsermüdung bei Nutzern durch seltenere Abfrage derselben Einwilligung
- Eindeutige Fälle, in denen Cookies ohne Einwilligung ausgeführt werden dürfen (zum Beispiel für aggregierte Zielgruppenmessungen durch First-Party-Daten)

Aber denken Sie daran: **Das ist ein Gesetzesentwurf, kein geltendes Gesetz.** Der Inhalt kann sich im Laufe des Gesetzgebungsverfahrens noch erheblich ändern. Viele wichtige **Interessenvertreter wie der Europäische Datenschutzausschuss (kurz EDSA) haben bereits Stellungnahmen und Empfehlungen veröffentlicht**.

Die Einführung des Gesetzes soll gestaffelt erfolgen und kann nach dem Inkrafttreten bis zu 48 Monate in Anspruch nehmen. Bis dahin gelten weiterhin die aktuellen DSGVO- und ePrivacy-Vorgaben. **Das heißt, Sie müssen Ihr Setup nicht sofort von Grund auf neu gestalten. Aber wenn Sie wissen, wohin die Reise geht, sind Sie besser vorbereitet und können schneller aktiv werden, wenn es so weit ist.**



Kurz und knapp: Was bedeutet der Digital Omnibus-Vorschlag für Vermarkter?

Das ist neu

Eindeutigere Regeln für Banner-Designs. Der Gesetzesentwurf sieht eine Ein-Klick-Option zum Ablehnen von Cookies vor, die genauso gut sichtbar und zugänglich ist wie der Button zum Annehmen. Dark Patterns sind untersagt. Wenn ein Nutzer die Einwilligung ablehnt, darf dieser mindestens sechs Monate lang nicht noch einmal abgefragt werden.

Mehr Klarheit bei First-Party-Analysen. Kumulierte Zielgruppenmessungen mit ausschließlich First-Party-Daten, bei denen keine Daten weitergegeben, weiterverkauft oder weiterverwendet werden, können unter bestimmten Voraussetzungen ohne Einwilligung durchgeführt werden.

Wichtige Einwilligungssignale (z. B. auf Browser- oder Betriebssystem-Ebene). Nutzer sollen Datenschutzeinstellungen einmalig vornehmen können. Diese Einstellungen werden dann automatisch an alle besuchten Websites übermittelt. Das bedeutet wiederum, dass Websites in der Lage sein müssen, diese Signale zu lesen, zu befolgen und ihr Tracking dementsprechend anzupassen.

Das bleibt unverändert

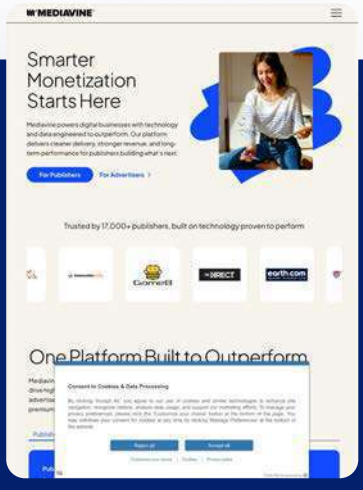
Opt-in-Optionen für Anzeigen und Tracking. Einwilligungen bleiben weiterhin die Standardlösung für Werbung, Profiling, seitenübergreifendes Tracking und die meisten Drittanbieter-Analysen. Das grundlegende Opt-in-Modell ändert sich nicht.

In der Praxis sähe das wie folgt aus: Einem Nutzer werden mit der Zeit seltener Banner ausgespielt. Im Hintergrund ist aber **trotzdem eine solide Einwilligungsinfrastruktur erforderlich.**

Ihre Nutzer sehen nur Ihr Banner. Was zählt, ist, wie Ihr System mit den Signalen umgeht, Regeln umsetzt und Einwilligungen mit Ihren Analysen, Werbeanzeigen und Kundenplattformen vernetzt.

Der Gesetzesentwurf sieht eine spezielle Ausnahme für Mediendienstanbieter vor. Unternehmen, deren Umsatz zu großen Teilen auf Werbeanzeigen fußt, sind ausdrücklich von der Pflicht ausgenommen, maschinenlesbare Präferenzsignale zu respektieren. Mehr dazu erfahren Sie **hier**.

Das signalisiert vor allem eins: Der Plan der EU ist auf Praktikabilität ausgelegt, nicht auf starre Strukturen. Das Ziel ist es, das System zu vereinfachen, nicht ganze Unternehmen lahmzulegen. Das ist ein gutes Zeichen dafür, dass der fertige Gesetzestext ein echtes Gleichgewicht zwischen Datenschutz und dem wirtschaftlichen Alltag schafft.



Unsere Experten-Vorhersage zur Zukunft der Cookie-Einwilligungen

„Einwilligungen sind mittlerweile viel mehr als nur eine einfache Compliance-Formalität. Sie sind ein neuer, rechtssicherer Weg, um Daten zu erfassen und zu verwenden.
Während Regulierungsrahmen weiterhin gültige, durchsetzbare Nutzerentscheidungen erfordern, hängt der Zugang zu Daten immer häufiger ausschließlich von Einwilligungen ab.
In diesem Zusammenhang wird die Fähigkeit, Einwilligungssignale zu erfassen, einzuordnen und umzusetzen, ein immer wichtigerer Faktor sowohl für die Compliance als auch für die Marketing-Performance."

Giulia Stancampiano,
Head of Legal (Privacy & Tech) bei iubenda

Neuer Mechanismus, gleiche Anforderungen

Einwilligungen werden nicht von heute auf Morgen verschwinden. Was sich ändert, ist, wie sie über mehrere Systeme hinweg umgesetzt, gespeichert und erteilt werden.
Mit den geplanten Präferenzsignalen auf Browser- oder Geräteebene können Nutzer ihre Datenschutzentscheidungen einmalig treffen und sie über verschiedene Websites hinweg anwenden lassen, anstatt bei jedem Besuch das gleiche Banner lesen zu müssen. **Es geht nicht darum, ob Einwilligungen erforderlich sind. Es geht darum, den Prozess zu optimieren.**

Damit das auch in der Praxis funktioniert, müssen einige Voraussetzungen erfüllt sein:

- Die Signale müssen mit den bestehenden Standards funktionieren (Interoperabilität).
- Die Signale müssen echte technische Funktionen für Websites und Dienste auslösen.
- Das Modell darf die Kontrolle nicht auf eine kleine Anzahl an Plattformen beschränken.

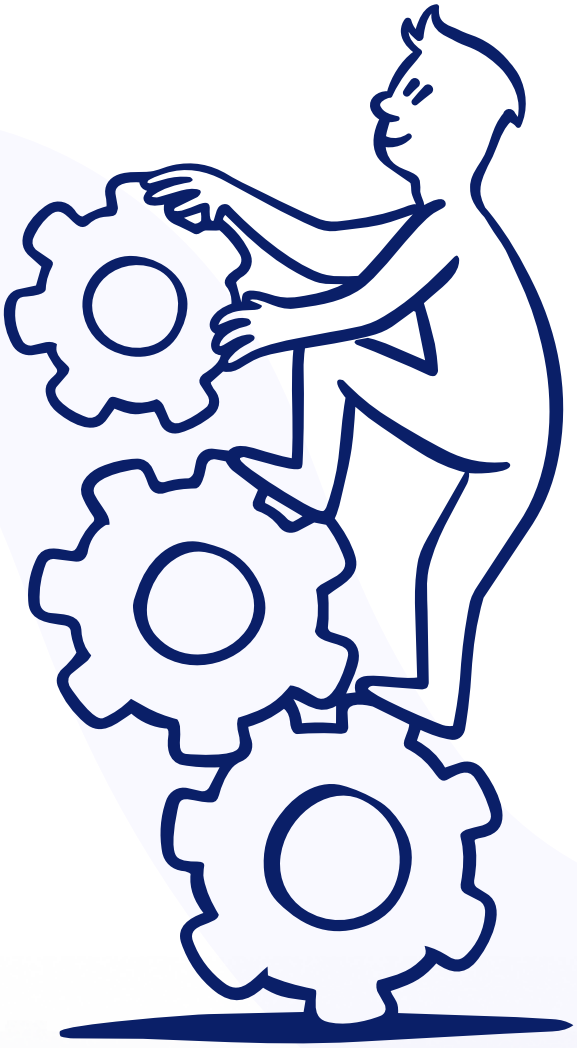
Das bedeutet für die Praxis: mehr vernetzte Systeme

Mit der Zeit werden den Nutzern weniger Banner ausgespielt, für die sie bereits eine Entscheidung getroffen haben. Der Prozess wird im Hintergrund dadurch jedoch keinesfalls entschlackt. Die Einwilligungsinfrastruktur existiert in einem umfassenderen, interoperablen Rahmenwerk. Das bedeutet, dass die Umsetzung komplexer wird durch:

- unterschiedliche Quellen für Einwilligungssignale (Banner, Browser, Apps),
- mehrere nachgeschaltete Systeme (Analysen, Werbeanzeigen, Datenplattformen),
- laufende Anforderungen für den Nachweis, die Umsetzung und die Nutzerkontrolle.

Ihre Consent Management Platform ist nicht nur eine Schnittstelle, die Ihre Einwilligungen erfasst. Ihr wird in diesem neuen Prozess eine wichtige Rolle zuteil. Vor allem mit dem Aufkommen neuer Signalquellen wird ihre Bedeutung immer wichtiger.
Signale auf Browser-Ebene werden Ihre CMP nicht ersetzen. Sie geben ihr neuen Input. Sie muss trotzdem über Ihren gesamten Tech-Stack Nutzerpräferenzen in echtes, durchsetzbares technisches Verhalten umsetzen, von Websites und Apps über Analysen bis hin zu Werbediensten.

Kurz gesagt, die Zukunft der Cookie-Einwilligung liegt darin, Einwilligungsmechanismen stärker miteinander zu vernetzen sowie kompatibler und reibungsloser zu gestalten.



Haftungsausschluss: In diesem E-Book geht es um einen Gesetzesentwurf, kein geltendes Gesetz. Der Inhalt gibt die Einschätzung von iubenda Stand März 2026 wieder und ist nicht als Rechtsberatung auszulegen. Wenden Sie sich an Ihren Rechtsbeistand für eine individuelle Beratung, die zu Ihrem Unternehmen passt.

Das macht erfolgreiche Vermarkter 2026 und darüber hinaus aus

Jene Vermarkter, die als Sieger hervorgehen, setzen auf ein solides Grundgerüst, das immer standhält -- egal, welche Gesetzänderungen beschlossen werden. Compliance ist der Ausgangspunkt. Wachstumsorientierte Vermarkter denken weiter und machen aus ihr einen Wettbewerbsvorteil.

Dieser Abschnitt widmet sich vier Bereichen, in denen Ihre Datenschutz-, Daten- und Einwilligungsprozesse einen direkten Einfluss auf Ihre Marketing-Performance haben können.

01 Compliance neu denken: Ihre Chance auf mehr Vertrauen

Was das bedeutet

Die meisten Marketing-Teams sehen Datenschutz-Compliance und Cookie-Einwilligungen als eigene Welt an: Das Rechtsteam legt die Regeln fest, das Produktteam baut das Banner und das Marketing-Team arbeitet innerhalb der vorgegebenen Grenzen. Aber dieser Ansatz kostet Sie bares Geld.

Denn in der Praxis müssen **Ihr Einwilligungs-Banner, Ihre Datenschutzerklärung und Ihre Datenprozesse** vom Marketing-Team fein aufeinander abgestimmt werden. Denn genau das sind die Elemente, die entscheidend für das Kundenvertrauen, die Kundengewinnung und die **Kundenbindung sind.**

Wenn Banner die Präferenzen Ihrer Besucher nicht umsetzen, Ihre Datenschutzerklärung schon seit Jahren nicht aktualisiert wurde oder Einwilligungsabläufe Ihre Nutzer eher frustrieren als ihnen Sicherheit geben, stehen Sie vor einem großen rechtlichen Problem. Und die Kosten sind nicht zu unterschätzen.

Laut einem Bericht des Marktforschungsunternehmens Ipsos gaben mehr als zwei Drittel (68 %) der Befragten an, dass sie der Art und Weise, wie Unternehmen ihre Daten zu Marketingzwecken verwenden, skeptisch gegenüberstehen. Lediglich 3 % der Befragten glaubten, dass sie online die volle Kontrolle über die Weitergabe und Löschung ihrer Daten haben.

Warum es funktioniert

Marketing-Teams, die Compliance die Aufmerksamkeit schenken, die sie verdient, erzielen bessere Ergebnisse. Keine Überraschungen mitten in der Kampagne, kein Analyse-Teardown, wenn sich herausstellt, dass Ihr Tracking-Setup nicht gesetzeskonform ist.

So drückt es **Adam Taylor, UK Privacy Lead bei Google Marketing Platform (GMP), im Interview mit The Drum aus:**

> „Datenschutz ist im Marketing schon lange kein Nischenthema mehr, sondern eine Schlüsselkompetenz. Und das macht sich in vielen Bereichen bemerkbar: wen Sie einstellen, wie Sie Ihre Mitarbeitenden und sich selbst schulen und fördern, wie Sie Entscheidungen zu Technologien und Partnern treffen und wie Sie effektiv über verschiedene Disziplinen und Funktionen hinweg kommunizieren."

Compliance als Infrastruktur und Vertrauensfaktor anzusehen bedeutet, wichtige Touchpoints von Beginn an darauf auszurichten - und diese nicht erst dann auszubessern, wenn Ihre Nutzer sich bereits ein Bild von Ihnen gemacht haben.

Genau das funktioniert, denn genau das wollen Ihre Besucher von Ihnen sehen. **Eine Verbraucherstudie zu Datenschutz und -sicherheit von Deloitte** fand heraus, dass

> „die Mehrheit der Befragten mehr Schutz und Kontrolle bei der Verwendung ihrer Daten wollen. Fast 9 von 10 Personen gaben an, dass es möglich sein sollte, Daten, die Unternehmen von ihnen erfassen, einzusehen und zu löschen."

Was Sie jetzt tun können

- **Versetzen Sie sich in Ihre Besucher.** Durchlaufen Sie Ihren Einwilligungsprozess als Nutzer, der Ihre Website zum ersten Mal besucht. Wo gibt es Unklarheiten, wo fühlt er sich aufdringlich an, wo könnte die Navigation verbessert werden? Das sind genau die Momente, an denen das Vertrauen Ihrer Nutzer zu bröckeln beginnt -- noch weit bevor es überhaupt aufgebaut wurde.

- **Prüfen Sie Ihr aktuelles Setup.** Erstellen Sie eine Map aller Tools, die Cookies ausführen und personenbezogene Daten verarbeiten. Untersuchen Sie, wo es Lücken zwischen Ihrem Banner und Ihrer Datenschutzerklärung gibt und was tatsächlich umgesetzt wird.

- **Machen Sie Compliance zum festen Bestandteil Ihrer Marketingprojekte.** Egal ob vor dem Launch einer neuen Kampagne, vor dem Kauf eines neuen Tools oder vor dem Erschließen eines neuen Markts: Führen Sie einen Compliance-Check durch.

„Viele Vermarkter sehen Compliance als Einschränkung an. Wir sehen sie als Chance, das Vertrauen unserer Kunden in unsere Marke zu stärken. Transparente Einwilligungen und verantwortungsbewusste Datenpraktiken führen zu besseren Kundenbeziehungen und schlussendlich auch zu besserer Performance. Genau deshalb hat sie bei team.blue und unseren mehr als 60 Marken so einen hohen Stellenwert.“

Shelby Torrence,
Group Marketing Director bei team.blue

Überprüfen Sie Ihre Compliance in Sekunden

Finden Sie heraus, ob Ihre Website die Vorschriften einhält – mit einem kostenlosen Scan.

URL einfügen und Compliance-Bericht sichern

02 Datenschutzsensible Messungen

Was das bedeutet

Datenschutzsensible Messungen bedeuten, einen datenschutzfreundlichen Ansatz für Ihre Marketing-Performance zu entwickeln, der präzise mit den Daten arbeitet, die Ihnen zur Verfügung stehen, und intelligent jene Daten nachbildet, die Ihnen fehlen.
Datenschutz und Datensicherheit sind dabei wichtiger als aufdringliches Tracking auf Einzelebene. Hier sind zwei wirkungsvolle datenschutzsensible Messstrategien, die Sie berücksichtigen sollten:

- **Google Consent Mode.** Wenn ein Nutzer die Einwilligung ablehnt, sendet der **Consent Mode** eingeschränkte Signale ohne Cookies, um Google zu ermöglichen, Conversions kumuliert nachzubilden. So wird sichergestellt, dass Messungen fortlaufend durchgeführt werden können. Die Signale gehen auf Google-Systemen wie Google Analytics ein, welche KI-Unterstützung nutzen, um Conversions von Nutzern einzuschätzen, die der Einwilligung widersprochen haben. Die Grundlage dafür ist das Nutzungsverhalten von Nutzern, die ihre Einwilligung erteilt haben.

- **Serverseitiges Tracking.** Serverseitiges Tracking entwickelt sich unter E-Commerce- und Marketing-Teams aktuell zur zuverlässigsten Messalternative. Anstatt das Tracking über den Browser der Nutzer laufen zu lassen, erfasst das serverseitige Tracking Ereignisse direkt auf dem Server und ordnet jeder Aktion eine servergenerierte ID zu, bevor die Signale an Analyse-Tools und Werbeplattformen weitergeleitet werden.

Weder serverseitiges Tracking noch der Google Consent Mode ersetzen die Pflicht einer gültigen Nutzereinwilligung. Beides sollte zusammen mit (und nicht als Ersatz für) Ihre Consent Management Platform (CMP) genutzt werden, welche die Entscheidungen Ihrer Nutzer erfasst und speichert.

Der Google Consent Mode ist beispielsweise ein Mechanismus, der anpasst, wie sich Google Analytics und Advertising Tags auf Grundlage der Nutzerpräferenzen verhalten, und gibt diese Präferenzen an Google-Dienste weiter. Ihre CMP sorgt dafür, dass Tags die Präferenzen Ihrer Nutzer respektieren.

Warum es funktioniert

Consent Mode ist mittlerweile im Europäischen Wirtschaftsraum und im Vereinigten Königreich Pflicht. Google begann im Juli 2025 damit, Werbefunktionen für Accounts einzuschränken, die den Google Consent Mode nicht aktiviert haben.

Die Conversion-Modellierung durch den Consent Mode stellt mehr als 70 % der Conversion-Klickpfade wieder her, die durch das Ablehnen von Cookies verlorengegangen sind. Diese Wiederherstellung bedeutet für Sie konkret genaueres Bidding, bessere Kampagnenoptimierung und ein deutlicheres Bild darüber, was Ergebnisse bringt -- und was nicht.

"Lange Zeit sah es so aus, als würden sich Werbetechnologie und Datenschutz in unterschiedliche Richtungen entwickeln. Dann haben wir den Google Consent Manager für unsere Kunden implementiert. Wenn Nutzer Cookies ablehnen, modelliert Google die entgangenen Conversions nach, unseren Bidding-Algorithmen stehen mehr Daten zur Verfügung und unsere Kampagnen performen besser. Datenschutz-Compliance und Ad Performance sind keine Gegensätze. Hat man die Tools einmal verstanden, können sie hervorragend zusammenarbeiten."

Virginie Rivet,
Senior GTM & Marketing Strategy Consultant bei Cremanski & Company

Was Sie jetzt tun können

- **Implementieren Sie den Google Consent Mode v2, wenn Sie das noch nicht getan haben (hier erfahren Sie, ob er für Ihre Website bereits aktiviert wurde).** Das ist der wichtigste Schritt, den Sie jetzt direkt umsetzen können. **Ihre CMP** muss gültige Einwilligungen erfassen und die Entscheidungen technisch umsetzen können. Besprechen Sie mit Ihrem Rechtsteam, ob fortgeschrittene Funktionen wie der Advanced Consent Mode (übermittelt Signale ohne Cookies vor der Einwilligung) oder Enhanced Conversion (übermittelt First-Party-Daten zur besseren Attribution an Google) für Ihr Unternehmen in Frage kommen.

- **Versuchen Sie es mit serverseitigem Tracking.** EU-Datenschutzvorschriften sind ständig im Wandel und es ist möglich, dass Browser-basiertes Tracking in Zukunft weiter eingeschränkt wird. Erfahren Sie mehr darüber, wie Ihnen serverseitiges Tracking zu verlässlicheren Messungen verhelfen kann.

- **Überprüfen Sie Ihre IAB TCF-Integration.** Wenn Sie programmatische Werbung schalten, bedeutet ein mangelhaft konfiguriertes TCF-Setup, dass Einwilligungssignale Ihren Tech-Stack nicht erreichen. Konkret heißt das: Nutzer, die eigentlich einer Einwilligung widersprochen haben, werden möglicherweise weiterhin getrackt.

03 First-Party-Daten: Ihr Ass im Ärmel

Was das bedeutet

Die Verwendung von First-Party-Daten zu überdenken ist ein kluger Schachzug für alle Vermarkter. First-Party-Daten haben sich zur zuverlässigsten Quelle für kanalübergreifende Leistung und Kundenbindung entwickelt.

First-Party-Daten sind jene Informationen, die Sie direkt von den Personen erfassen, die mit Ihrem Unternehmen interagieren, zum Beispiel Anmeldungen, Käufe, Einstellungen und Verhalten auf der Website.

Warum es funktioniert

Alles steht und fällt mit Transparenz. Wenn Ihre Kunden verstehen, wie ihre Daten verwendet werden, und die Kontrolle über ihre Daten behalten, sind die Daten, die Sie erfassen, genauer, zuverlässiger und dadurch umso wertvoller.

1

Transparenz bei jedem Touchpoint

Ihre Cookie-Richtlinie, Ihr Preference-Center und Ihr Opt-out-Prozess sind nicht bloß rechtliche Vorgaben. Sie sind das erste Zeichen für Ihre Kunden, dass ihre Daten bei Ihnen in sicheren Händen sind. Achten Sie darauf, dass sie so eindeutig wie möglich, leicht zugänglich und einfach zu bedienen sind.

2

Ihre Kunden willigen bewusst ein

Wenn Ihre Nutzer verstehen, wozu sie ihre Einwilligung geben, und Ihnen vertrauen, dass Sie ihre Entscheidung respektieren, sind sie eher geneigt, ihre Daten mit Ihnen zu teilen, weil sie die Kontrolle über ihre eigenen Daten behalten. Genau das macht First-Party-Daten so wertvoll.

3

Ihnen stehen mehr Daten zur Verfügung

Daten, die nach einer ausdrücklichen Einwilligung erfasst wurden, spiegeln echtes Interesse wider. Das ist um Welten zuverlässiger als Daten, die über Drittanbieter-Tracking erfasst werden, und hält auch den sich ändernden Datenschutzvorschriften stand.

4

Ihr Marketing wird intelligenter

Erfahren Sie, was Ihrer Zielgruppe wirklich wichtig ist und wer echtes Interesse hat. Sparen Sie sich Ausgaben für Tools und Maßnahmen, die nicht funktionieren, und optimieren Sie Ihr Targeting.

5

Sie bieten eine individuelle Nutzererfahrung

Geben Sie Ihren Kunden, was Sie wirklich wollen. Wenn Sie verstehen, wie ihre Zielgruppe tickt, können Sie jede Phase der Customer Journey individuell gestalten und stärkere Bindungen aufbauen.

6

Verbesserte Marketing-Performance und mehr Umsatz

Kunden, die ihre Einwilligung geben, fühlen sich respektiert und wissen, dass sie die Kontrolle über ihre Daten behalten. Und eine relevante Nutzererfahrung sorgt dafür, dass Ihre Besucher eher bei Ihnen kaufen und bleiben. Bessere Daten bedeuten für Sie weniger unnötige Ausgaben, mehr Conversions, bessere Bindungsraten und nachhaltigen Mehrwert für Ihre Kunden.

Das Ergebnis ist ein Kreislauf, von dem alle profitieren. Das gestärkte Vertrauen wirkt sich auf beide Seiten aus: auf Ihre Marketing-Daten und auf Ihre Kundschaft. First-Party-Daten sind eine Wachstumsstrategie.

Ein Branchenbericht von Deloitte aus dem Jahr 2023 zu First-Party-Daten, der von Meta in Auftrag gegeben wurde, ergab:

> **„82 % der Marktführer** nutzen First-Party-Daten, um einen unmittelbaren Mehrwert für ihre Kunden zu schaffen“, mit Fokus auf Transparenz. Führende Marken informieren ihre Kunden darüber, wie ihre Daten zur Unterstützung wichtiger Aufgaben verwendet werden.
>
> Aus dem gleichen Bericht geht hervor, dass Unternehmen, die in maßgeschneiderte, datengestützte Nutzererfahrungen investieren:
>
> - **einen 27%igen Anstieg** der Konversionsrate und
> - einen **23%igen Anstieg** bei der Kundenzufriedenheit feststellten.
>
> Deloitte Digital for Meta

„Datenschutz-Compliance wird oft als rechtliche Verpflichtung abgetan. Wir sehen das anders. Sie ist eine Chance, eine echte Verbindung mit ihrer Zielgruppe aufzubauen: Lassen Sie Ihre Nutzer über ihre Daten entscheiden und respektieren Sie diese Entscheidung – die Vorteile kommen von ganz allein.“

Diana Dee Rabba,
VP of Marketing bei Accessiway

Was Sie jetzt tun können

- **Identifizieren Sie die Datenpunkte, die für Entscheidungen wirklich wichtig sind.** Konzentrieren Sie sich dabei auf Signale, die mit Ihren Zielen in Verbindung stehen: E-Mail-Anmeldungen, Bestellverläufe, Produktvorlieben. Wenn Sie wählerisch sind, erfassen Sie zwar weniger; aber das, was Sie erfassen, ist umso nützlicher.
- **Geben Sie Ihren Nutzern einen Grund dafür, ihre Einwilligung zu geben.** Der Mehrwert muss klar und deutlich erkennbar sein. „Erhalten Sie exklusiven Frühzugang zu neuen Produkten“ ist aussagekräftiger als „besseres Nutzererlebnis“.
- **Entwickeln Sie ein Preference-Center.** Bieten Sie Ihren Nutzern eine einfache Seite, auf der sie ihre Kommunikationspräferenzen, E-Mail-Häufigkeit und Datenschutzentscheidungen jederzeit aktualisieren können.
- **Vernetzen Sie Ihren Einwilligungsprozess mit Ihren Tools.** Ihr Banner sollte das kontrollieren, was aus Ihren Analysen und Werbeplattformen hervorgeht. Ihre CMP setzt das dann automatisch um.
- **Nutzen Sie First-Party-Daten, um Ihre Datenmodellierung zu verbessern.** Wenn Sie Ihre Kundenliste in die Plattformen von Meta oder Google einspeisen, verbessert sich dadurch die Zielgruppenqualität, vor allem mit abnehmenden Drittanbieter-Signalen.

04 Einwilligungsrate: So holen Sie das Beste raus

Was das bedeutet

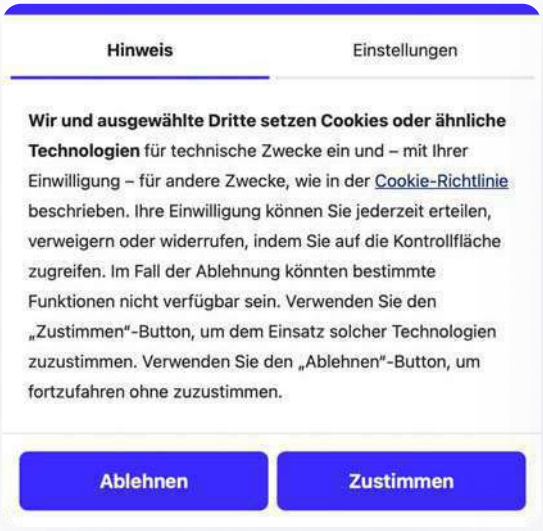
Die Einwilligungsrate ist die Prozentzahl an Nutzern, die aktiv Cookies akzeptieren (Opt-in). Sie schafft es nur selten auf die Marketing-Performance-Agenda. Dabei bietet sie tiefe Einblicke.

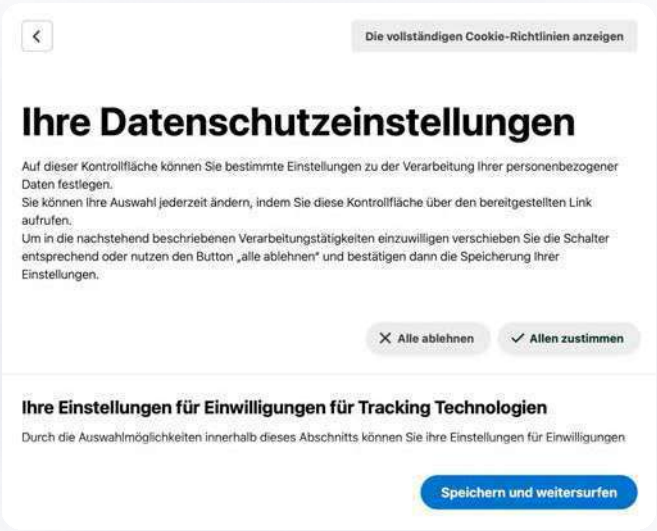
Denn jeder Prozentpunkt mehr bedeutet:

- mehr sichtbare Conversions,
- mehr zielgerichtete Attribution,
- bessere Bidding-Signale und mehr Gewinn pro Werbeanzeige.
- einen höheren Return on Advertising Investment.

Ihre Einwilligungsrate lässt sich durch ein besseres Banner-Design, deutlichere Sprache, eine geeignete Position und Wiederherstellungsprozesse für Nutzer, die zunächst keine Einwilligung erzielen, verbessern.

Warum es funktioniert





Wussten Sie, dass Ihr Banner-Design und insbesondere die Position des Banners einen messbaren Einfluss hat? **Unsere eigenen Daten** zeigen, dass die Einwilligungsrate durch ein Banner am Seitenanfang im Gegensatz zum Seitenende um 16 % steigt. Ein Logo sorgt für mehr Vertrauen und gesteigerte Opt-in-Raten.

Mangelhaftes UX-Design

- Buttons zum Annehmen oder Ablehnen von Cookies in unterschiedlichen Größen oder Farben
- Option zum Ablehnen in sekundärem Menü versteckt
- Keine Möglichkeiten zur Anpassung der Präferenzen nach dem ersten Besuch
- Banner wird bei jeder Session neu angezeigt
- Kein Branding auf dem Banner
- Lange Banner-Ladezeit

Besseres UX-Design

- Buttons zum Annehmen oder Ablehnen in gleicher Größe und gut sichtbar
- Beide Optionen gut sichtbar direkt im ersten Menü
- Preference-Center jederzeit durch ein Widget zugänglich
- Einwilligung wird über mehrere Sessions hinweg gespeichert und nach einem angemessenen Zeitraum erneut abgefragt
- Logo gut erkennbar, Design passt zum Rest der Website
- Banner lädt schnell und beeinträchtigt nicht die Website-Performance

Was Sie jetzt tun können

Kümmern Sie sich als Erstes um das Grundlegende: Ihr Banner muss schnell laden und darf die Leistung Ihrer Website nicht stören. Ein langsames oder gar aufdringliches Banner führt dazu, dass Ihre Besucher Ihre Website verlassen, bevor sie überhaupt die Einwilligungsoptionen gesehen haben. Sie können keine Rate optimieren, die von Beginn an keine echte Chance hatte.

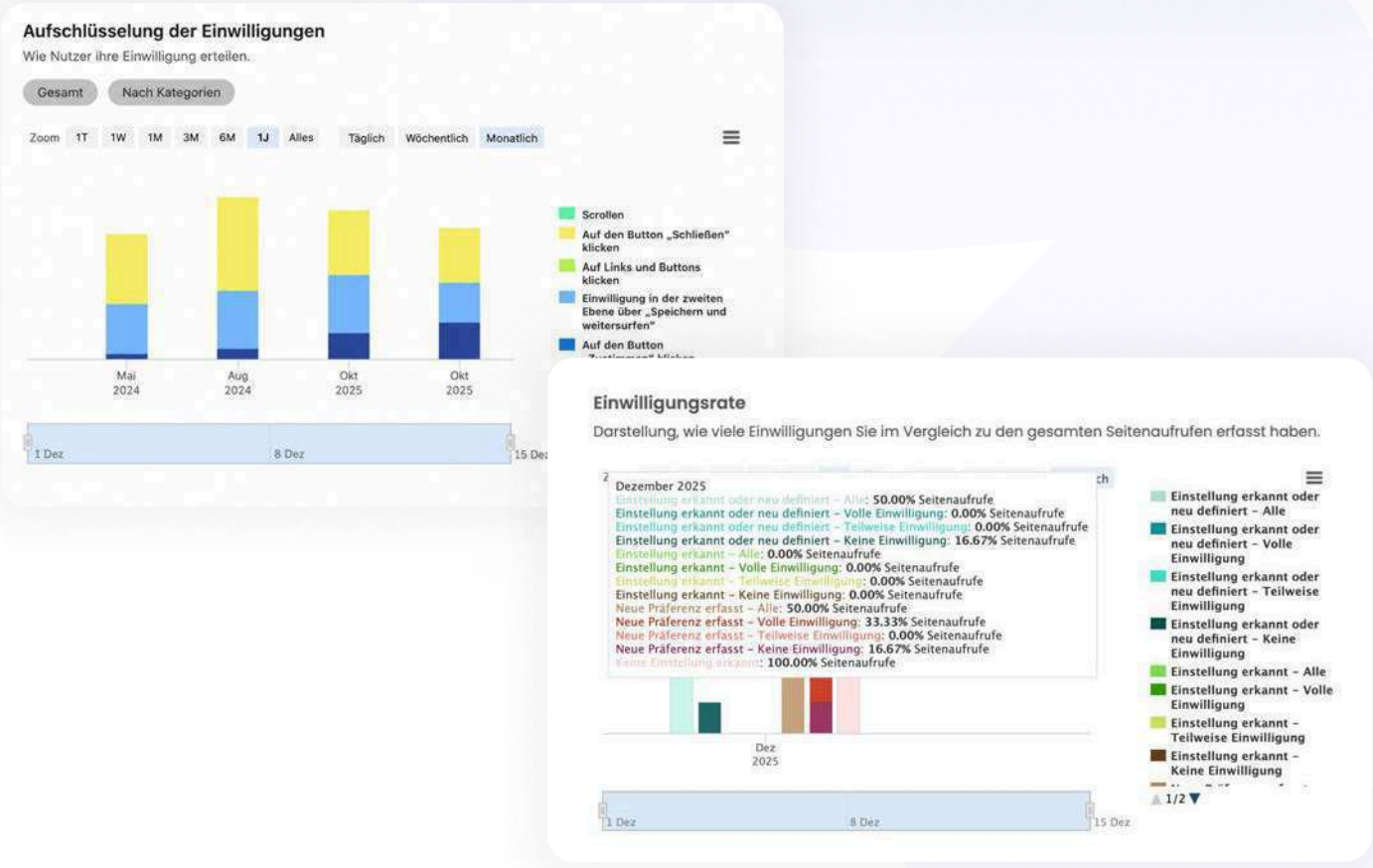
- **Überprüfen Sie Ihre aktuelle Einwilligungsrate.** Wenn Sie diese Kennzahl bisher noch nicht messen, sollten Sie damit jetzt anfangen. Ihr CMP-Dashboard sollte Ihnen Ihre Opt-in-Raten je nach Gerät, Land und Bannerposition zeigen.

- **Führen Sie einen A/B-Test für Ihr Banner durch.** Testen Sie verschiedene Positionen, Schaltflächenbeschriftungen und Texte. Selbst kleinste Änderungen können Ihre Rate erheblich beeinflussen.

- **Verwenden Sie einen Prozess zur Rückgewinnung von Einwilligungen.** Mit unserer **Rückgewinnung nach Ablehnung** können Sie Nutzern, die zunächst keine Einwilligung gegeben haben, innerhalb des gesetzlich zulässigen Rahmens eine nachgeschaltete Meldung senden.

- **Stimmen Sie Ihr Banner-Design auf Ihre Marke ab.** Durch ein auf Ihre Marke abgestimmtes Banner fühlen sich Ihr Banner und Ihre Website wie aus einem Guss an. Je stimmiger das Gesamtbild, desto eher interagieren Ihre Nutzer bewusst mit Ihrem Banner, anstatt es zu ignorieren.

- **Überprüfen Sie Ihr Mobilerlebnis separat.** Einwilligungsraten fallen auf Mobilgeräten häufig anders aus als auf dem Desktop. Testen Sie beides.



Teams, die jetzt aktiv werden, haben die Nase vorn

> „Wenn Einwilligungen, Datenschutz und Compliance ab dem ersten Tag mitgedacht werden, können Produkt-, Marketing- und Wachstumsteams sich schneller und sicher weiterentwickeln. Sie testen mehr, versenden mehr und scheitern bei Ihrem Wachstum nicht an der gläsernen Decke.“
>
> 
> Andreea Maria Mandeal,
> **CMO, iubenda**

Teams, die frühzeitig aktiv werden, haben einen wichtigen Vorsprung. Sie hinterfragen Annahmen, testen kontinuierlich und sehen Compliance als festen Bestandteil ihrer Marketing-Infrastruktur an – nicht als rechtliche Formalität.

Egal, wie es mit den Regeln rund um Cookie-Einwilligungen weitergeht, vorausschauende Vermarkter fangen mit dem an, was sie heute umsetzen können.

💡 Datenschutzbestimmungen werden nicht von heute auf Morgen verschwinden. Für Teams, die nachhaltig entwickeln, ist sie keine lästige Einschränkung, **sondern ein wichtiger Filter, mit dem sichtbar wird, welche Marken sich das Vertrauen ihrer Kunden verdient haben – und welche nicht.**

Ihr Partner für Compliance und Wachstum

iubenda hilft Unternehmen seit 2011 dabei, sich im Datenschutz-Dschungel zurechtzufinden - lange bevor die DSGVO überhaupt ein fester Begriff war. Heute vertrauen uns über 150.000 Unternehmen weltweit. Wir entwickeln Tools, die Ihnen komplexe Rechtsaufgaben abnehmen, damit Sie sich auf Ihre Performance konzentrieren können.

Entwickelt mit Fachexperten

Unser Rechtsteam hat Datenschutzbestimmungen schon lange, bevor sie Einzug in den Mainstream erhalten haben, verfolgt. Unser **Generator für Datenschutz- und Cookie-Richtlinien** erstellt entsprechend globaler Datenschutzgesetze Rechtsdokumente, einschließlich DSGVO in Europa oder CCPA in den USA. Aktualisieren Sie Ihre Compliance-Dokumente und -Prozesse jederzeit mit nur wenigen Klicks.

Analysen für mehr Wachstum

- **Erfassen Sie Ihre Einwilligungsrate** je nach Gerät, Kategorie und Land.
- **Führen Sie A/B-Tests** an Ihren Banner-Designs durch oder holen Sie mit dem consentmanager von iubenda **First-Party-Daten** ein, um herauszufinden, was dazu führt, dass mehr Besucher einwilligen.
- **Nutzen Sie die Rückgewinnung nach Ablehnung**, um Nutzern, die ihre Einwilligung nicht gegeben haben, zu einem passenden Zeitpunkt erneut um ihre Einwilligung zu bitten. Jeder Prozentpunkt, um den Ihre Einwilligungsrate ansteigt, bedeutet bessere Daten, genauere Attribution und effizientere Werbeanzeigen und Targeting.

Tools, die wirklich Zeit sparen

Entwickeln Sie ein vollständig konfiguriertes Einwilligungs-Banner mit Preference-Center, erstellen Sie Rechtsdokumente und verbinden Sie Ihre Einwilligungssignale mit Ihren Analysen und Werbeplattformen -- alles an einem Ort. Unsere **Privacy Controls & Cookie Solution**:

- bietet flexible Banner-Layouts und UX-Designs,
- lädt schnell und beeinträchtigt nicht Ihre SEO,
- blockiert Skripts bis zur Einwilligung.

Google-zertifizierter CMP-Partner mit eingebautem Consent Mode.

IAB-validierte CMP mit Unterstützung des Transparency & Consent Framework (TCF).

Mehr als 400.000
Seiten und Apps vertrauen auf uns

27
Sprachen (keine KI-Übersetzungen)

Jetzt kostenlos loslegen

Schreiben Sie uns

iubenda

Gebaut für Compliance.
Entwickelt für Wachstum.

Integrationen für alle wichtigen CMS: