Verbraucherzentrale
Hamburg

Cookie-Banner: Was Sie vor dem Klicken wissen sollten

Kaum eine Webseite kommt heute noch ohne Cookie-Banner aus. Viele klicken deshalb genervt auf „Alle akzeptieren“, einfach um möglichst schnell zum eigentlichen Inhalt zu gelangen. Dabei geht es um weit mehr als einen lästigen Hinweis. Cookie-Banner sollen sicherstellen, dass Sie selbst entscheiden können, welche Daten beim Surfen verarbeitet werden dürfen und welche nicht.



© Glenn Carstens Peters on Unsplash

DAS WICHTIGSTE IN KÜRZE

1. Cookies sind kleine Textdateien, die Webseiten auf Ihrem Endgerät speichern. Manche sind technisch notwendig, andere dienen Analyse-, Tracking- oder Werbezwecken.

2. Technisch notwendige Cookies dürfen auch ohne Einwilligung gesetzt werden. Für alle anderen Cookies ist grundsätzlich Ihre ausdrückliche Einwilligung erforderlich.
3. Cookie-Banner müssen Verbraucherinnen und Verbrauchern eine echte Wahl ermöglichen. Manipulative Gestaltungstricks, sogenannte Dark Patterns, sind häufig unzulässig.
4. Mit datenschutzfreundlichen Browser-Einstellungen und einem bewussten Umgang mit Cookie-Bannern lässt sich die Privatsphäre besser schützen.

Stand: 08.07.2026

Cookie-Banner sollen die gesetzlichen Vorgaben zum Datenschutz und zum Schutz der Privatsphäre umsetzen. Webseiten müssen Nutzerinnen und Nutzer grundsätzlich um ihre Einwilligung bitten, bevor nicht technisch notwendige Cookies auf dem Endgerät gespeichert oder ausgelesen werden. In der Praxis gelingt das allerdings nicht immer.

Was sind Cookies?

Cookies sind kleine Textdateien, die beim Besuch einer Webseite im Browser Ihres Computers, Tablets oder Smartphones gespeichert werden. Sie helfen einer Webseite beispielsweise dabei, einen Warenkorb zu speichern, einen Login wiederzuerkennen oder bestimmte Einstellungen zu merken.

Cookies sind deshalb nicht grundsätzlich problematisch. Entscheidend ist, welchem Zweck sie dienen.

Manche Cookies werden automatisch gelöscht, sobald Sie den Browser schließen. Andere bleiben über längere Zeit gespeichert.

Welche Cookies sind notwendig?

Notwendige Cookies sind für grundlegende Funktionen einer Webseite technisch erforderlich. Dazu gehören beispielsweise der Warenkorb in einem Online-Shop, die Anmeldung im Kundenkonto, Spracheinstellungen oder Sicherheitseinstellungen.

Häufig handelt es sich dabei um sogenannte Session-Cookies. Sie werden automatisch gelöscht, sobald der Browser geschlossen wird. Für diese Cookies ist keine Einwilligung erforderlich.

Welche Cookies sind nicht notwendig?

Daneben gibt es Cookies, die für die eigentliche Nutzung einer Webseite nicht erforderlich sind. Sie dienen dazu, das Verhalten von Nutzerinnen und Nutzern über verschiedene Webseiten hinweg nachzuvollziehen. Sie werden beispielsweise eingesetzt, um Reichweiten zu messen, das Surfverhalten auszuwerten, personalisierte Werbung anzuzeigen oder Nutzerinnen und Nutzer wiederzuerkennen.

Für diese Cookies ist grundsätzlich Ihre ausdrückliche Einwilligung erforderlich.

Lehnen Sie diese Cookies ab, sollten Sie die Webseite grundsätzlich trotzdem nutzen können. Nur in besonderen Ausnahmefällen kann ein Angebot von einer Einwilligung abhängig gemacht werden.

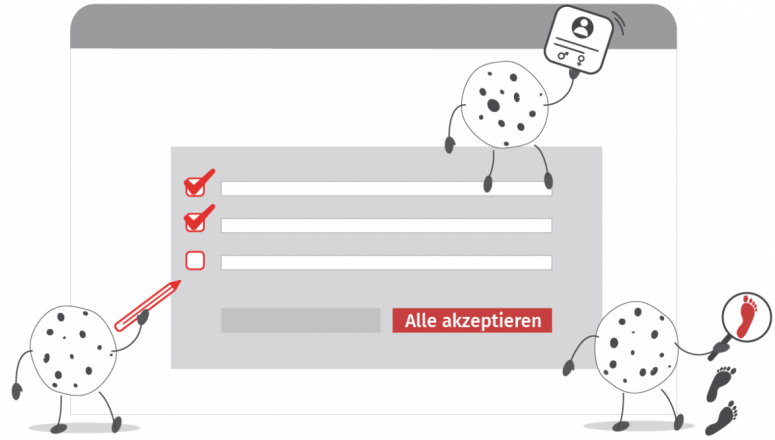
Was sind Drittanbieter-Cookies?

Nicht alle Cookies stammen von der Internetseite, die Sie gerade besuchen.

Drittanbieter-Cookies werden beispielsweise von Werbe- oder Analyseunternehmen gesetzt. Sie ermöglichen häufig, Nutzerinnen und Nutzer über verschiedene Webseiten hinweg wiederzuerkennen. Dadurch entstehen detaillierte Interessen- und Nutzungsprofile, die unter anderem für personalisierte Werbung genutzt werden.

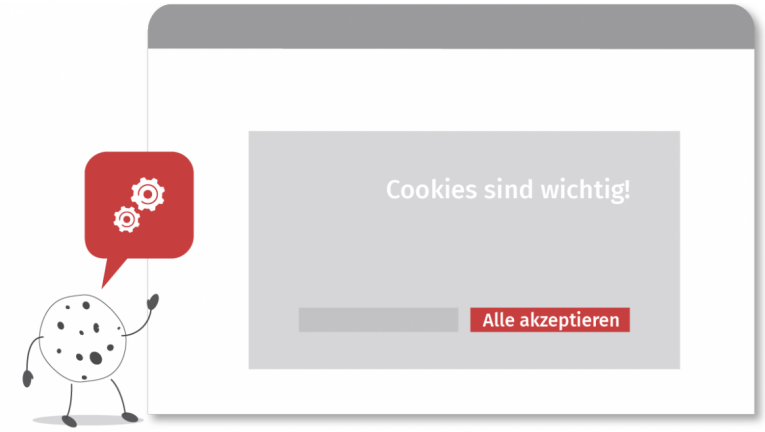
Für Verbraucherinnen und Verbraucher ist oft kaum nachvollziehbar, welche Unternehmen ihre Daten erhalten und wie diese weiterverarbeiten.

Manche Webseiten berufen sich zusätzlich auf sogenannte berechtigte Interessen. Dabei geht es um bestimmte Datenverarbeitungen nach der Datenschutz-Grundverordnung (DSGVO). Das ersetzt jedoch grundsätzlich nicht die erforderliche Einwilligung für das Speichern oder Auslesen nicht technisch notwendiger Cookies auf Ihrem Endgerät.



Bei diesem Banner gibt es zwar Auswahlmöglichkeiten, aber die Cookies, die personenbezogene Daten speichern, sind schon ausgewählt. Diese Art von Cookie-Bannern ist unzulässig, weil man bereits ausgewählten Cookies aktiv ablehnen müssen.

© verbraucherzentrale.de



Bei diesem Banner hat man Auswahlmöglichkeiten und es sind keine Haken gesetzt. Allerdings ist das Banner so gestaltet, dass man dazu verleitet wird, auf „akzeptieren“ zu klicken. Ein „Ablehnen“-Button ist nur durch einen Klick auf Einstellungen sichtbar. Nach Auffassung der Verbraucherzentralen sollten auch solche Banner verboten sein.

© verbraucherzentrale.de

GUT ZU WISSEN

Cookies spielen beim Tracking im Internet zwar eine wichtige Rolle. Sie sind heute aber längst nicht mehr die einzige Technik, mit der Informationen über das Surfverhalten gesammelt werden. Webseiten nutzen zunehmend auch andere Verfahren, zum Beispiel:

- **Browser-Fingerprinting:** Beim Browser-Fingerprinting werden verschiedene technische Merkmale Ihres Geräts und Browsers kombiniert, etwa Betriebssystem, Browsertyp, Bildschirmauflösung oder installierte Schriftarten. Daraus kann ein individueller „Fingerabdruck“ entstehen, mit dem Ihr Gerät wiedererkannt wird. Anders als bei Cookies wird dabei keine Datei auf Ihrem Endgerät gespeichert.
- **Tracking-Pixel:** Tracking-Pixel sind winzige, meist unsichtbare Grafiken, die beim Besuch einer Webseite oder beim Öffnen einer E-Mail geladen werden. Sie können beispielsweise erkennen, ob eine E-Mail geöffnet oder eine Webseite besucht wurde.
- **Tracking-Skripte:** Viele Webseiten binden Programme ein, die das Verhalten ihrer Besucherinnen und Besucher auswerten. Sie erfassen beispielsweise, welche Seiten aufgerufen werden, wie lange ein Besuch dauert oder welche Inhalte besonders häufig angeklickt werden.

Deshalb reicht es nicht aus, nur auf Cookies zu achten. Wer möglichst datensparsam surfen möchte, sollte zusätzlich den Tracking-Schutz seines Browsers aktivieren und die Datenschutzeinstellungen regelmäßig überprüfen.

Welche Sicherheitsrisiken bestehen?

Cookies selbst sind in der Regel keine Schadsoftware. Sie übertragen keine Viren und infizieren keinen Computer.

Datenschutzrisiken entstehen vor allem durch Tracking-Cookies. Sie können umfangreiche Informationen über Ihr Surfverhalten sammeln. Werden diese Daten mit weiteren Informationen zusammengeführt, können sehr detaillierte Nutzerprofile entstehen. Diese werden unter anderem genutzt, um personalisierte Werbung auszuspielen oder Nutzerverhalten auszuwerten. Dadurch können Unternehmen sehr genaue Rückschlüsse auf Interessen, Gewohnheiten oder Kaufabsichten ziehen.

In seltenen Fällen können außerdem gestohlene Sitzungs-Cookies dazu genutzt werden, bestehende Anmeldungen zu übernehmen.

Worauf sollte man bei Cookie-Bannern achten?

Cookie-Banner sollen Ihnen eine freie Entscheidung ermöglichen. In der Praxis arbeiten jedoch viele Webseiten mit sogenannten Dark Patterns. Diese sollen Sie in eine bestimmte Richtung lenken, damit Sie zustimmen und einwilligen, selbst wenn das für Sie nicht vorteilhaft ist und Sie viele persönliche Daten preisgeben. Typische Beispiele dafür sind:

- besonders auffällige Schaltflächen wie „Alle akzeptieren“,
- versteckte oder schwer auffindbare Ablehnmöglichkeiten,
- mehrere Klicks bis zur Ablehnung, während „Alle akzeptieren" sofort auswählbar ist,
- irreführende Beschriftungen wie „Speichern“ statt „Ablehnen“,
- lange und unübersichtliche Texte, die eine informierte Entscheidung erschweren,
- voreingestellte Häkchen für Marketing- oder Statistik-Cookies.

Die Schaltflächen zum Akzeptieren und Ablehnen sollten gleichwertig gestaltet sein. Das Ablehnen darf nicht deutlich umständlicher sein als das Akzeptieren.

Unser **interaktives Dark-Patterns-Spiel** zeigt mit einem Augenzwinkern, mit welchen Gestaltungstricks Webseiten arbeiten können und worauf Sie achten sollten.

Einfach den roten Start-Button drücken und los geht's. Aber lassen Sie sich nicht täuschen! Wenn es Ihnen mal zu schnell geht, einfach den Pause-Button drücken. **Viel Glück und viel Spaß beim Spiel!**

Lösungen fürs Dark-Patterns-Spiel

Lösung 1: Ablehnen

Anbieter versuchen durch optische Täuschungen und unternehmensfreundliche Voreinstellungen Ihre Einwilligung zu bekommen. So werden bewährte Designs ausgenutzt, um Sie vom richtigen Weg abzubringen. Drücken Sie den überdimensionalen Zustimmungsbutton, erhält der Anbieter der Webseite viele persönliche Daten von Ihnen.

Lösung 2: Kreuz oben rechts anklicken (Kreuz = ablehnen)
Auch hier wird der Fokus auf den Einwilligungsbutton gelenkt. Oft verstecken Anbieter die Möglichkeit abzulehnen auf ihrer Webseite. Achten Sie deswegen auf versteckte Hinweise oder suchen Sie sich einen anderen Anbieter.

Lösung 3: Ablehnen (rot)
Schon als Kind lernen wir, dass man nur bei grün über die Straße gehen darf. Die Farbe löst bei uns das Gefühl aus, die richtige Entscheidung zu treffen. Manche Anbieter nutzen diese einstudierten Verhaltensmuster, um Sie mit ihrem manipulativen Design von der richtigen Entscheidung abzulenken.

Lösung 4: Ablehnen
Der grüne Button springt hin und her. Einige Anbieter versuchen mit auffälligen grafischen Elementen vom Inhalt abzulenken und zu verwirren. Lassen Sie sich davon nicht austricksen und in die Irre führen.

Lösung 5: Decline
„Decline“ ist Englisch und bedeutet übersetzt ablehnen. Können Sie wichtige Informationen nur in einer Fremdsprache abrufen, dann sollten Sie nur eine Entscheidung treffen, wenn Sie den Inhalt auch verstehen und eine selbst bestimmte Entscheidung treffen können. Anderenfalls lass en Sie lieber die Finger davon.

Lösung 6: Klicke auf das Wort „Freund:in“ im Text.
Einen solchen Cookie-Hinweis werden Sie in der Realität sicher nicht finden. Es gibt jedoch Anbieter, die versuchen, Sie mit Trickfragen zu täuschen und Ihnen eine Zustimmung zu entlocken. Am besten ist es, solche Angebote zu vermeiden.

Lösung 7: 16
Klaus wird mitgezählt. Er ist ja schließlich auch ein Lebewesen. Klar, dieses Beispiel werden Sie im wahren Leben ebenfalls nicht finden, Trickfragen und versteckte Informationen aber schon.

Lösung 8: 1. Schritt: Bitte nicht hier klicken. 2. Schritt: Versteckt im Fließtext findest du den Hinweis „Cookies ablehnen“. Da musst du klicken.
Nicht selten verstecken sich relevante Informationen im Fließtext. Wenn Ihnen Ihre persönlichen Daten wichtig sind, dann nehmen Sie nicht die Abkürzung und stimmen allem zu. Lassen Sie sich Zeit, lesen Sie die versteckten Hinweise und treffen Sie dann deine Entscheidung.

Lösung 9:

1. Cookie Menü durch Klick ausklappen
2. Cookies-Rezepte auswählen
3. Schoko-Cookies auswählen
4. Sonstige Cookies Menü ausklappen
5. Sonstige Cookies auswählen
6. Nein anklicken

Oft werden relevante Informationen auch in komplexen Untermenüs versteckt. Solche Strukturen sollen Sie davon abhalten, die richtige Wahl zu treffen. Doch bedenken Sie: Nur zwei Klicks mehr und Ihre Daten sind sicher!

Lösung 10: Ja, ich hasse süße Tiere.
Manche Anbieter wollen Sie mit emotionalen Formulierungen unter Druck setzen und Ihnen damit eine Zustimmung entlocken. Lassen Sie sich von dem Spiel mit Ihren Emotionen nicht einfangen und täuschen.

Lösung 11: „Ja“ klicken.
Auch verwirrende Trickfragen mit doppelten Verneinungen oder missverständlichen Formulierungen haben nur ein Ziel: Unklarheit schaffen und Sie zu einer falschen Entscheidung verleiten. Finden Sie solche Hinweise, lassen Sie lieber die Finger von dem Anbieter.

Lösung 12: Ablehnen
Gezielte Hindernisse wie lange Klickwege sollen Sie dazu bringen, die einfache Variante zu wählen und allem zuzustimmen. Manchmal lenken auch auffällige grafische Elemente vom Inhalt ab. Bei dieser Variante wird das Warten belohnt. Brechen Sie vorschnell ab und stimmen allem zu, dann geben Sie Ihre persönlichen Daten frei.

Lösung 13: Alle 6 Ampelfelder auswählen.
Hindernisse können in verschiedenen Varianten auftreten. Ein hier zu sehendes „Captcha“ ist eigentlich ein Test, ob es sich bei den Nutzerinnen und Nutzern um einen Menschen oder einen Roboter / ein Computerprogramm handelt. So soll der Zugriff insbesondere von Spam-Programmen und Bots erschwert werden. Alle zeitraubenden,

unternehmensfreundlichen Voreinstellungen sollen Sie regelmäßig davon abhalten, Ihre Zustimmung zu verweigern. Machen Sie es den Anbietern nicht leicht und gehen Sie den Umweg.

Lösung 14: Die voreingestellten Haken entfernen und stattdessen „Nein, Danke“ anklicken.

Auch hier gilt: Lassen Sie sich nicht beirren. Anbieter wissen, dass Sie keine Lust auf ellenlanges Scrollen haben. Sie gestalten den „Klickweg“ extra lang, damit Sie die schnellere, unternehmensfreundliche Variante wählen. Davon sollten Sie sich nicht abhalten lassen. Wählen Sie nicht den einfachen, voreingestellten, sondern den längeren Weg. Entfernen Sie die Haken und verweigern Sie die Zustimmung. Oder: Suchen Sie sich einen anderen Anbieter!

Lösung 15: Schnell die Haken entfernen und „Nein, Danke“ auswählen.

Aufgepasst! Jetzt heißt es schnell sein, denn die einmal entfernten Haken kommen wieder. Lassen Sie sich davon nicht abhalten und bleiben Sie bei Ihrer Entscheidung. „Nein, danke“ ist und bleibt die richtige Antwort.

Lösung 16: Wiederholt „Ablehnen“ auswählen und bei der Entscheidung bleiben.

Immer wiederkehrende Hinweise sollen Sie nerven und dazu bringen, dass Sie irgendwann einfach zustimmen, um Ihnen das Wegklicken zu ersparen. Hier heißt es einfach standhaft bleiben und immer wieder ablehnen.

Lösung 17: 82

Zugegeben, auch diese vielleicht etwas kniffelige Aufgabe wird dir im wahren Leben bei einem Cookie-Hinweis nicht begegnen. Hindernisse, die Ihnen auf dem Weg zur richtigen Entscheidung in den Weg gelegt werden, gibt es jedoch zahlreiche. Ist Ihnen z.B. schon einmal aufgefallen, dass ein Account sehr leicht abgeschlossen, aber nur schwer wieder gekündigt werden kann?

Lösung 18: Alle Cookies auf deinem Bildschirm müssen einzeln weggeklickt werden.

Bei dieser Variante werden Sie anhand des Designs dazu gezwungen, eine Handlung vorzunehmen, um sich vor Cookies zu schützen. Es kommt häufig vor, dass Cookie-Banner nicht richtig oder nicht in Gänze gelesen werden können und dadurch eine freie Entscheidung beeinflusst wird. Meiden Sie Anbieter, die solche Anwendungen nutzen.

Lösung 19: Der Keks muss immer wieder angeklickt werden, bis er verschwindet.
Auch hier werden Sie gezwungen, eine Handlung vorzunehmen (Cookie anklicken), um die gewünschte Handlung (Cookies ablehnen) vorzunehmen.

Lösung 20: Abbrechen
Falsche und irreführende Informationen, verbunden mit einem manipulativen Design sollen Sie in diesem Fall dazu bringen, die Zustimmung zum Setzen von Cookies zu erteilen. Klickt man den Button „Erneut versuchen“, werden nicht die Cookie-Hinweise geladen. Vielmehr wird bereits die Zustimmung erteilt. Hier hilft nur genaues Lesen.

Lösung 21: Ich möchte kein Gewinner sein.
Es gibt Anbieter, die bei mehreren Auswahlmöglichkeiten eine Variante bewusst in einem abwertenden, negativen Tonfall formulieren. Auf diesem Weg wollen sie Sie davon abhalten, die „richtige“ Wahl zu treffen. Wer will schon schuld daran sein, dass man den Gewinn verpasst.

Lösung 22: Nummer ziehen und im Wartebereich Platz nehmen. Hierzu mit der Maus auf den runden Knopf klicken und den Mauszeiger über das graue Feld „Wartebereich“ schieben. Ein Countdown beginnt dann automatisch zu laufen.
Auch bei diesem Beispiel wird man über eine Voreinstellung des Anbieters gezwungen, eine Handlung vorzunehmen, um zu dem gewünschten Erfolg zu gelangen.

Lösung 23: Klicke auf die AGB, nach unten scrollen und „Ablehnen“ auswählen.
Achtung! Hier stimmt man nicht den Allgemeinen Geschäftsbedingungen zu, sondern dem Setzen von Tracking-Cookies. Ein bewährtes Design – die Zustimmung zu Allgemeinen Geschäftsbedingungen – wird ausgenutzt, um in die Irre zu führen. Lassen Sie sich keinen Bären aufbinden und lehnen Sie ab.

UNSERE TIPPS

Sie müssen nicht automatisch jedem Cookie-Banner zustimmen. Mit wenigen Einstellungen können Sie Ihre Privatsphäre beim Surfen besser schützen. Wir empfehlen:

- Akzeptieren Sie möglichst nur notwendige Cookies.
- Klicken Sie nicht vorschnell auf „Alle akzeptieren“.

- Aktivieren Sie den Tracking-Schutz Ihres Browsers. Viele moderne Browser verfügen bereits über integrierte Schutzfunktionen, die sich in den Datenschutzeinstellungen aktivieren lassen.
- Blockieren Sie nach Möglichkeit Drittanbieter-Cookies.
- Löschen Sie Cookies regelmäßig über die Browser-Einstellungen.
- Nutzen Sie Browser-Erweiterungen (auch Add-ons genannt). Das sind kleine Zusatzprogramme, die nachträglich im Browser installiert werden und beispielsweise Werbung, Tracker oder Cookie-Banner automatisch blockieren können (zum Beispiel der Nervenschoner“ der Verbraucherzentrale Bayern).
- Verwenden Sie ausschließlich Erweiterungen aus vertrauenswürdigen Quellen.
- Nutzen Sie den privaten oder Inkognito-Modus, wenn Sie weniger Spuren auf Ihrem eigenen Gerät hinterlassen möchten. Er macht das Surfen jedoch nicht anonym und schützt nur eingeschränkt vor Tracking durch Webseiten.

Die Grafiken auf dieser Seite sind im Rahmen eines vom Bundesministerium der Justiz und für Verbraucherschutz geförderten Projekts entstanden.

Gefördert durch:

Bundesministerium
der Justiz und
für Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

© Verbraucherzentrale Hamburg e. V.

https://www.vzhh.de/themen/telefon-internet/datenschutz/cookie-banner-was-sie-vor-dem-klicken-wissen-sollten