Cookies

geschrieben von Tobias Hager | 3. August 2025



Cookies: Die Wahrheit über die kleinen Datenkrümel im Web

Cookies sind kleine Textdateien, die Websites im Browser eines Nutzers speichern, um Informationen über dessen Aktivitäten, Präferenzen oder Identität zu speichern. Sie gehören zum technischen Rückgrat des modernen Internets – oft gelobt, oft verteufelt, meistens missverstanden. Ob personalisierte Werbung, bequeme Logins oder penetrante Cookie-Banner: Ohne Cookies läuft im Online-Marketing fast gar nichts. In diesem Glossar-Eintrag zerlegen wir das Thema Cookies bis auf die letzte Byte-Ebene – ehrlich, kritisch und ohne Schönfärberei.

Autor: Tobias Hager

Cookies erklärt: Definition, Funktionsweise und Typen

Cookies sind winzige Textpakete, die von Websites an den Browser gesendet und dort lokal gespeichert werden. Bei jedem folgenden Zugriff auf dieselbe Website sendet der Browser diese Informationen zurück an den Server. So entsteht ein Zustand – eine Art Gedächtnis im ansonsten zustandslosen HTTP-Protokoll. Die Technik ist so alt wie das Web selbst, aber immer noch hochgradig relevant – und umstritten.

Man unterscheidet grundsätzlich zwischen zwei Haupttypen von Cookies:

- First-Party-Cookies: Diese werden direkt von der besuchten Website gesetzt. Sie sind essenziell für Logins, Warenkörbe, Spracheinstellungen und Benutzererlebnisse. Ohne sie wäre E-Commerce auf dem Level von 1995.
- Third-Party-Cookies: Sie stammen von externen Anbietern, also Domains, die nicht mit der besuchten Seite identisch sind. Typisch für sie: Tracking, Retargeting und Analyse über mehrere Websites hinweg. Genau diese Cookies sind der Grund, warum du nach dem Schuhkauf überall Schuhwerbung siehst.

Technisch betrachtet bestehen Cookies aus einem Namen, einem Wert, einem Ablaufdatum (Expiration Date), einem Pfad, einer Domain und optional Flags wie Secure (nur über HTTPS übertragen) und HttpOnly (nur für Server, nicht für JavaScript zugänglich). Diese Parameter bestimmen, wie, wann und wem die Cookies übermittelt werden.

Die Funktionsweise ist simpel, aber mächtig: Setzt eine Website ein Cookie, wird dieses bei jedem weiteren Request an diese Website automatisch mitgeschickt. So lassen sich Nutzer wiedererkennen, Sessions verwalten, Präferenzen speichern oder – weniger charmant – Nutzerprofile für Werbung erstellen.

Cookies im Online-Marketing: Tracking, Targeting und Consent

Im Online-Marketing sind Cookies das Schweizer Taschenmesser für alles, was mit Nutzerverfolgung, Personalisierung und Conversion-Optimierung zu tun hat. Ohne Cookies wären Webanalyse, Remarketing und A/B-Testing ein Blindflug.

Die wichtigsten Einsatzbereiche im Marketing:

- Session-Management: Speichern von Login-Zuständen, Warenkörben und Spracheinstellungen. Ohne Cookies müsste man nach jedem Klick von vorn beginnen.

- Webanalyse: Tools wie Google Analytics oder Matomo setzen Cookies, um wiederkehrende Besucher, Verweildauer oder Conversion-Pfade zu erfassen. Ohne diese Daten wäre datengetriebenes Marketing ein Märchen.
- Tracking und Retargeting: Third-Party-Cookies ermöglichen es Werbenetzwerken (z. B. Google Ads, Facebook Pixel), Nutzer über verschiedene Websites hinweg zu verfolgen. So entstehen detaillierte Nutzerprofile, die für personalisierte Werbung genutzt werden.
- A/B-Testing und Personalisierung: Cookies sorgen dafür, dass Nutzer konsistent die gleiche Variante einer Website sehen oder personalisierte Inhalte ausgespielt bekommen.

Mit der DSGVO und der ePrivacy-Richtlinie ist die Cookie-Welt allerdings komplexer und nerviger geworden. Consent-Management-Plattformen (CMPs) regeln, ob und welche Cookies gesetzt werden dürfen. Ohne explizite Zustimmung darf kaum noch ein Tracking-Cookie gesetzt werden – was Marketer zur Verzweiflung und Banner-Allergie treibt. Die Folge: Cookie-Banner, Consent-Layer und sinkende Datenqualität.

Für die technisch Interessierten: Cookies sind nicht die einzige Tracking-Technologie, aber immer noch die weitverbreitetste. Alternativen wie Local Storage, Session Storage oder Fingerprinting existieren, werden aber ebenfalls zunehmend kritisch beäugt.

Sicherheit, Datenschutz und das Cookie-Sterben: Herausforderungen für Unternehmen

Cookies sind nicht nur nützlich, sondern auch ein potenzielles Sicherheits- und Datenschutzrisiko. Cross-Site Scripting (XSS) kann Cookies abgreifen, wenn sie nicht richtig konfiguriert sind. Das HttpOnly-Flag schützt immerhin vor Zugriff durch JavaScript, das Secure-Flag vor Abgriff über unverschlüsselte Verbindungen. Dennoch: Wer Cookies falsch einsetzt, öffnet Hackern und Datensammlern Tür und Tor.

Datenschützer hassen Cookies – zumindest die, die Nutzer ohne Einwilligung verfolgen. Die DSGVO verlangt explizite Einwilligung für alle nicht-technisch notwendigen Cookies. Das hat zu einer regelrechten Cookie-Banner-Seuche geführt, bei der viele Nutzer genervt auf „Akzeptieren“ klicken, ohne zu wissen, was sie tun. Für Unternehmen bedeutet das: Ohne sauberes Consent-Management drohen Abmahnungen und Strafen.

Das Cookie-Sterben ist in vollem Gange. Apple (Safari) und Mozilla (Firefox) blockieren Third-Party-Cookies standardmäßig, Google zieht mit Chrome bald nach. Die Werbeindustrie sucht verzweifelt nach Alternativen – etwa serverseitiges Tracking, kontextbasierte Werbung oder die viel diskutierte

Google Privacy Sandbox. Eines ist sicher: Die goldenen Zeiten der grenzenlosen Nutzerverfolgung sind vorbei.

Einige Best Practices für den sicheren und datenschutzkonformen Einsatz von Cookies:

- Nur technisch notwendige Cookies ohne Consent setzen
- Alle anderen Cookies erst nach expliziter Einwilligung
- Klare, verständliche Cookie-Policies veröffentlichen
- HttpOnly und Secure-Flags konsequent nutzen
- Regelmäßige Audits und Anpassung an neue Rechtsprechung

Cookies und SEO: Auswirkungen auf Sichtbarkeit und Nutzererfahrung

Cookies sind für SEO kein direkter Rankingfaktor, aber sie beeinflussen die Nutzererfahrung und damit indirekt das Ranking. Ein Cookie-Banner, das den Content verdeckt oder die Seite verlangsamt, sorgt für höhere Absprungraten – Google merkt das und straft ab. Besonders kritisch: Cookie-Layer, die Googlebot aussperren oder das Crawling behindern. Hier trennt sich die Spreu vom Weizen.

Auch für die technische SEO gibt es Fallstricke. Werden Sessions oder wichtige Inhalte nur nach Setzen von Cookies ausgeliefert, sieht der Googlebot – der keine Cookies akzeptiert – nur leere Seiten. Das Ergebnis: Indexierungsprobleme und Sichtbarkeitsverlust. Saubere Implementierung ist Pflicht, kein Nice-to-have.

Wer international unterwegs ist, muss zusätzlich auf unterschiedliche Gesetzeslagen achten. Was in Deutschland als technisch notwendig gilt, kann in Frankreich oder den USA anders bewertet werden. Wer hier schludert, riskiert schlechte Rankings, rechtliche Probleme und Vertrauensverlust bei Nutzern.

Die wichtigsten Tipps für SEO- und Conversion-optimierte Cookie-Nutzung:

- Consent-Banner möglichst schlank, schnell und nicht-invasiv gestalten
- Crawler-Zugriff auf Hauptinhalte nie durch Cookie-Layer blockieren
- Technisch notwendige Cookies klar trennen und sauber dokumentieren
- User Experience immer über reine Datensammelwut stellen

Fazit: Cookies sind tot – lang

leben Cookies (und Alternativen)

Cookies sind die Dinosaurier des Webs – technisch simpel, aber immer noch allgegenwärtig. Für Marketer, SEOs und Datenschützer sind sie Fluch und Segen zugleich. Mit dem Aussterben der Third-Party-Cookies beginnt eine neue Ära des datenschutzfreundlichen, aber auch datenärmeren Marketings. Wer jetzt nicht umdenkt, landet digital auf dem Abstellgleis.

Die Zukunft? Serverseitiges Tracking, Identifier-Lösungen, kontextbasierte Ausspielung und ein bewusster Umgang mit Nutzerdaten. Wer Cookies weiterhin sinnvoll, sicher und transparent einsetzt, gewinnt das Vertrauen der Nutzer und bleibt wettbewerbsfähig. Wer dagegen auf veraltete Methoden setzt, wird von Browsern, Gesetzgebern und Nutzern gleichermaßen abgestraft. Willkommen im neuen Zeitalter der Datensparsamkeit – die Cookie-Party ist vorbei, aber das Web lebt weiter.