Was sind Third Party Cookies?

Stand: 17.10.2022

Werbetreibende nutzen Third Party Cookies, um damit über Werbeschaltungen auf anderen Seiten Nutzerinformationen in Form von Datensätzen zu sammeln. Diese werden im Browser des Nutzers gespeichert, damit dieser bei einem erneuten Besuch einer Webseite mit der Werbung des gleichen Anbieters wiedererkannt wird. Mit Third Party Cookies lässt sich nachvollziehen, welche Wege ein Nutzer im Internet geht. Das ermöglicht Werbetreibenden, auf das Nutzerprofil exakt zugeschnittene Werbung auszuspielen.

Unterschied zwischen First Party und Third Party Cookie

First Party Cookies lassen sich normalerweise direkt zum Webseitenbetreiber zurückverfolgen, während Third Party Cookies von einer anderen Seite, einer dritten Person, stammen, die ihre Cookies zu Werbezwecken auf anderen Seiten platzieren.

Nutzerdaten werden über Cookies direkt vom Webseitenbetreiber als auch von einem Werbetreibenden, der auf der besuchten Seite Werbung für wiederum seine eigene Webseite macht, gesammelt. Daten, die über First Party Cookies gespeichert werden, werden nur von der Seite des Webseitenbetreibers, der diese Cookies implementiert hat, erkannt. Weitergegeben an Dritte werden sie nicht.

Third Party Cookies sind technisch einfach einzubinden. Im Vergleich zu First Party Cookies muss nämlich auf der Seite, auf der die Cookies arbeiten sollen, kein Code hinterlegt werden. Eine Werbeanzeige vom AdServer des Drittanbieters reicht hier aus.

Umfangreiche Nutzerprofile erstellen

Im Wesentlichen sammeln Werbetreibende mithilfe von Third Party Cookies Informationen über Webseitenbesucher, um daraus abzuleiten, wofür diese sich innerhalb einer Domain sowie über diese hinweg interessieren. Damit werden dann Nutzerprofile erstellt, für die dann gezielt Werbung gezeigt werden kann.

Gesammelt werden unter anderem:

- Verweildauer
- Seitenaufrufe
- Bewegung des Nutzers über Links

Third Party Cookies – das Problem mit dem Datenschutz

Insbesondere in Deutschland sind die Datenschutzrichtlinien streng. Daher wird der Einsatz von Third Party Cookies von Datenschützern stark kritisiert, denn diese Art der Datensammlung ist nicht anonym. Im Fokus der Kritik steht vor allem, dass Nutzerdaten über andere Seiten hinweg gesammelt werden und Dritte

darauf zugreifen können.

Mittlerweile gibt es eine europäische Richtlinie, die sogenannte E-Privacy-Richtlinie, wie persönliche Daten verarbeitet, gespeichert, genutzt und weitergegeben werden müssen. Laut der E-Privacy-Richtlinie müssen Nutzer proaktiv über eine Opt-in/Opt-out-Funktion zustimmen, damit die Daten getrackt werden dürfen.

In Deutschland wurde diese Richtlinie noch nicht umgesetzt. Unter anderem, weil es immer noch unklar ist, welche Vorschriften für deutsche Webseiten gelten. Im Grunde aber ist eine Umsetzung der europäischen Richtlinie nicht notwendig, da bereits die deutsche Rechtslage durch das Telemediengesetz TMG genau diese Vorgaben erfüllt. Wer als Webseitenbesitzer auf der rechtlich sicheren Seite sein möchte, integriert eine Opt-out-Funktion entlang der TMG-Richtlinien.

Die Alternativen zu Third Party Cookies

Zunehmend wird nach Alternativen zu Third Party Cookies gesucht. Einerseits, weil Browser und Sicherheitseinstellung diese blockieren, andererseits, weil deren Akzeptanz immer weiter sinkt und zudem nicht für mobile Geräte nutzbar sind. Es gibt eine Reihe an Alternativen, die die Privatsphäre besser schützen und auf mobilen Endgeräten funktionieren – unter anderem das Fingerprinting. Hier wird ein Gerät anhand von individuellen Merkmalen wiedererkannt und entsprechend so das Nutzerverhalten im Internet nachvollziehbar.

Und auch Google arbeitet an einer Alternative, der sogenannten Google AdID. Diese soll für Werbetreibende anonym Daten sammeln. Wenn ein Nutzer auch diese nicht möchte, kann ein privater Modus eingeschaltet werden. Auf diese Weise werden keinerlei Informationen an Webseitenbetreiber und Werbetreibende weitergegeben.