

Analyse-Cookies sind verboten, wir brauchen etwas Neues! – Ist Online-Tracking DSGVO-konform ohne Einwilligung möglich?

Cookies sollten das Internet nutzerfreundlicher machen, indem Sie das Surfverhalten erfassen und Webseiten sowie Suchfunktionen darauf abstimmen. Allerdings geht es den meisten Unternehmen nicht nur um die reine Optimierung der Funktionsweise ihrer Website, denn diese ist ohne eine datenschutzrechtliche Einwilligung machbar, sondern auch um die Analyse des Nutzerverhaltens. Dass Letzteres nicht stillschweigend mit den geltenden Datenschutzbestimmungen einhergeht, hat das Urteil vom 28. Mai 2020 – I ZR 7/16 – Cookie-Einwilligung II des BGH¹ noch einmal bestätigt. Demnach sind ein Tracking und der Einsatz von Third Party-Cookies im Internet ohne eine aktive Einwilligung nicht mehr möglich.

Das wäre also endlich das von vielen Nutzern herbeigesehnte Ende der nervigen und unerwünschten Werbung im Internet, oder etwa doch nicht? Es heißt ja immer, dass Werber kreativ sind und wer besonders kreativ ist, arbeitet bei einem global tätigen Werbeunternehmen. Einige Werbeunternehmen bedienen sich des altbekannten Fingerprintings in neuen Abwandlungen. Google geht sogar noch einen Schritt weiter und versucht sich derzeit an seiner neuen Personalisierungstechnik FloC.

Aber was genau passiert dabei eigentlich, und wie verspricht man sich hierbei Datenschutzkonformität?

Beim Fingerprinting (Browser Fingerprinting oder Device Fingerprinting) wird, wie der Name schon vermuten lässt, ein individueller Abdruck der Nutzereinstellung und seinem Browsingverhalten erstellt. Dabei werden auf dem Endgerät gespeicherte Informationen ausgelesen. Dies können Schriftarten, Auflösung, Plugins, Browsertyp, Zeitzone, Hersteller und Typbezeichnung des Gerätes selbst und auch die IP-Adresse sein. Diese Daten werden auf dem Server des jeweiligen Webseitenbetreibers gespeichert und beim nächsten Aufruf der Seite mit den vorher gespeicherten Daten abgeglichen.

Um bei diesem Vorgehen datenschutzkonform zu handeln, sollen die Daten um die personenbezogenen Parameter gekürzt werden. Dabei soll dann unter anderem auf die IP-Adresse und alle Daten, die einen direkten Personenbezug zulassen, verzichtet werden. Dies soll am Ende einen Datenpool hervorbringen, der nicht auf eine natürliche Person zurückschließen lässt. Gleichet man allerdings die übrigen gesammelten Daten ab, kann mit einer hohen Wahrscheinlichkeit ein Profil von einem definierten Endgerät erstellt werden. Wenn man dieses Gerät jetzt noch mit einer eigenen ID versieht, kennt man zwar nicht den Namen des Nutzers oder wo genau sich dieser aufhält, aber man weiß, was der Nutzer des definierten Endgerätes bevorzugt. Darauf aufbauend kann ein Profil zu Werbezwecken erstellt werden, ohne eine Einwilligung zu benötigen, wie es bei Cookies der Fall ist. Ein Zustand, der sehr kritisch zu betrachten ist.

Google geht, als global tätiges Werbeunternehmen, einen Schritt weiter und ist derzeit dabei, zielgerichtete Werbung noch datenschutz-„freundlicher“ zu machen². Eine sog. „Privacy Sandbox“ soll neben den Third Party-Cookies auch das Fingerprinting unterbinden. Hierzu wird die hauseigene Personalisierungs-

technik FLoC API eingesetzt. FLoC (Kurzform für Federated Learning of Cohorts) soll das Surfverhalten des Nutzers auf dem lokalen System nachverfolgen und anhand der daraus abgeleiteten Interessen den Nutzer in eine Kohorte (Nutzergruppe) eingliedern. Hierbei wird nur der Kohorte eine ID gegeben und nicht einem einzelnen Gerät. Diese Kohorten sollen dann mit Werbetreibenden geteilt werden, um zielgruppengerichtete Werbung für die Nutzergruppe zu ermöglichen. Google bewirbt mit einem Whitepaper³, dass Rückschlüsse auf den jeweiligen Nutzer durch die Vielzahl an Nutzern in einer Kohorte erschwert werden („hide in the crowd“). Je mehr, desto sicherer – je weniger, desto genauer? Auch hierbei stehen am Ende wieder Fragen zur Datenschutzkonformität im Raum. Derzeit ist FLoC zwar noch nicht in Europa verfügbar, wird anscheinend aber in naher Zukunft über Googles Browser Chrome seinen Weg zu uns finden.

Am Ende zeigt sich hierbei wieder einmal, dass Datenschutz ein lebendes Konstrukt ist, das sich stetig in Bewegung befindet. Wann immer ein Gesetz oder ein Urteil es dem Datensammler schwieriger machen möchte, mutiert dieser zu einem mehr oder wenig kreativen Jäger auf der Suche nach neuen (derzeit noch erlaubten) Jagdgründen in den Weiten des World Wide Web.

Quelle:

1. <https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020067.html?nn=10690868>
2. <https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/>
3. <https://github.com/google/ads-privacy/blob/master/proposals/FLoC/FLoC-Whitepaper-Google.pdf>



Wichtiger Ratgeber.

Abmahnung, Einstweilige Verfügung und neues Wettbewerbsrecht

von Dr. Jürgen Niebling, Rechtsanwalt, Olching

2021, 4., überarbeitete Auflage, 104 Seiten, € 15,90

Das Recht der Wirtschaft, Band 240

ISBN 978-3-415-06922-0



Leseprobe unter

www.boorberg.de/9783415069220

BOORBERG

RICHARD BOORBERG VERLAG FAX 07 11/73 85-100 · 089/43 61 564
TEL 07 11/73 85-343 · 089/43 60 00-20 BESTELLUNG@BOORBERG.DE

SC0521