von Rechtsanwalt **Dr. Daniel S. Huber**

# Vorsicht: Die Nutzung von Facebook Custom Audiences ist datenschutzrechtlich problematisch - Was tun?

Mit dem Marketingtool Custom Audiences von Facebook können Händler potentielle Interessenten und Kunden ihrer Produkte oder Dienstleistungen recht zielgerichtet und somit vergleichsweise effizient bewerben. Allerdings ist der Einsatz des Tools datenschutzrechtlich problematisch und umstritten. Zwar werden personenbezogene Daten durch ein Hashing-Verfahren verfremdet, bevor sie verarbeitet werden. Doch findet nach Ansicht der Datenschutzbehörden dennoch eine Verarbeitung von personenbezogenen Daten statt, so dass datenschutzrechtliche Vorgaben zu beachten sind. Wir erläutern in diesem Beitrag, was beim Einsatz von Facebook Custom Audiences aus datenschutzrechtlicher Sicht zu beachten ist.

## I. Was ist Facebook Custom Audiences?

Facebook Custom Audiences bezeichnet Zielgruppen, an die gezielt Werbung auf Plattformen wie Facebook oder Instagram ausgespielt werden kann. Eine solche Werbezielgruppe kann etwa durch Kundendaten oder ein sog. Facebook-Pixel erstellt werden. Bei letzterem werden Personen, die durch ihre Nutzung der Plattform ein bestimmtes Pixel ausgelöst haben, beispielsweise eine bestimmte Datei innerhalb der letzten zwei Wochen heruntergeladen haben, automatisch in die Kundenliste aufgenommen.

Bei ersterem ist die Besonderheit, dass die für die Erstellung einer Custom Audience relevanten Daten von dem werbenden Unternehmen bei Facebook hochgeladen werden können, um die Zielgruppe für die eigene Werbung zu bestimmen. Bei diesen Daten handelt es sich meistens um eine Liste von Bestandskunden samt den entsprechenden Kundendaten, wie etwa Email-Adressen oder Telefonnummern.

## II. Werden im Rahmen von Facebook Custom Audiences personenbezogene oder anonyme Daten verarbeitet?

Ob es sich bei solchen Daten um personenbezogene Daten handelt, lässt sich auf den ersten Blick nicht eindeutig sagen. Denn Facebook benutzt bei der Erstellung von Custom Audiences das Hashing-Verfahren zur Maskierung von Daten und lehnt deshalb eine Einstufung der verwendeten (gehashten) Daten als personenbezogene Daten ab.

Um die datenschutzrechtliche Problematik bei Facebook Custom Audiences zu verstehen, muss man verstehen, was hinter dem Hashing-Verfahren steckt: Der Hashwert wird durch die sog. Hashfunktion

berechnet und ist das Ergebnis der Umwandlung einer Datei (und dessen Inhalts) in eine bestimmte Zeichenfolge mit fester Länge. Den Vorgang dieser Umwandlung in einen, oft kürzeren, numerischen Wert bezeichnet man dabei als „Hashing“. Wichtig zu wissen ist außerdem, dass es sich bei der Hashfunktion um eine Einwegfunktion handelt, was bedeutet, dass aus dem erzeugten Hashwert nicht auf den ursprünglichen Inhalt geschlossen werden kann.

Man muss sich die Erstellung von Facebook Custom Audiences durch Kundendaten somit folgendermaßen vorstellen:

- Das werbende Unternehmen hat die Möglichkeit, die Kundendaten, wie etwa Email-Adressen, in Facebook hochzuladen, allerdings nicht als Klartext, sondern in einer gehashten Form. In dieser Form ist es Facebook grundsätzlich auch nicht möglich, die originalen Klardaten, also Email-Adressen oder Telefonnummern zu ermitteln.
- Nachdem die gehashten Daten an Facebook übermittelt worden sind, erfolgt durch Facebook ein Abgleich zwischen den übermittelten Hashwerten und den bereits bei Facebook vorhandenen Hashwerten aller Facebook-Nutzer, welche Facebook aus den von den Nutzern angegebenen Daten für sich berechnet. Eine eventuelle Übereinstimmung bedeutet somit, dass eine von dem werbenden Unternehmen aufgelistete Person bereits einen Facebook-Account besitzt und daher auf der Facebook-Plattform gezielt beworben werden kann. Diese Übereinstimmungen werden dann im Kunden-Account des werbenden Unternehmens als „Custom Audience“ gespeichert und die betroffenen Kunden dadurch zielgerichtet beworben.

Bei der Erstellung von Custom Audiences erhält Facebook aber letztlich Informationen darüber, welche Facebook-Nutzer – also welche konkreten, d.h. auch identifizierbaren Kunden von Facebook - auch zu dem Kundenkreis des werbenden Unternehmens gehören oder in dessen elektronische Werbung eingewilligt haben. Bei diesen Informationen handelt es sich um personenbezogene Daten, weshalb auch das vorgelagerte Hashing zu keiner wirklichen Anonymisierung führt.

## III. Wieso wird Hashing auch nicht als taugliches Verfahren zur Anonymisierung von personenbezogenen Daten akzeptiert?

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), also die bayerische Datenschutzbehörde, kam bereits in der Berichtsperiode 2013/2014 zu dem Ergebnis, dass jedenfalls das Hash-Verfahren MD5 im Allgemeinen ungeeignet ist, um personenbezogene Daten zu anonymisieren.

Dabei wurde u.a. argumentiert, dass die durch die Hashwerte vermeintlich anonymisierten personenbezogenen Daten mit einer sog. „Brute-Force-Attacke“ wiederhergestellt werden könnten. Etwas vereinfacht dargestellt handelt es sich bei einer solchen Attacke um ein Ausprobieren möglichst vieler Email-Adressen und/ oder Telefonnummern. So banal dies auch klingen mag, kann ein solcher Angriff sehr wohl zur De-Anonymisierung der gehashten Daten führen, da die durch das MD5-Verfahren gehashten Daten in der Regel nach einem ähnlichen Schema aufgebaut sind.

Auch noch später in den Jahren 2015 und 2016 hielt das BayLDA an seiner Auffassung fest und hatte sowohl die Verfahren der Kundenliste als auch die des Zählpixels als datenschutzrechtlich problematisch eingestuft.

## IV. Ist eine datenschutzkonforme Nutzung von Facebook Custom Audiences überhaupt möglich?

Der Einsatz von Facebook Custom Audiences ist datenschutzrechtlich somit insgesamt zwar nicht unproblematisch. Händler können auf dieses Marketingtool aber dennoch zurückgreifen, wenn sie ein paar datenschutzrechtliche Aspekte im Blick behalten.

Eine Möglichkeit besteht darin, von den betroffenen Kunden eine datenschutzrechtliche Einwilligung hinsichtlich der Datenverarbeitung im Zusammenhang mit Facebook Custom Audiences einzuholen. Dabei sollte die Einwilligung – wie sämtliche datenschutzrechtlichen Einwilligungen – in transparenter Weise eingeholt und revisionssicher dokumentiert werden, um die rechtlichen Anforderungen an eine Einwilligung in die Weitergabe und Verarbeitung von Daten zu Werbezwecken bestmöglich zu erfüllen. Auch sollte nicht vergessen werden, die Datenschutzerklärung diesbezüglich anzupassen, insbesondere auch hinsichtlich des Hinweises auf die Widerrufsmöglichkeit des Kunden.

Ohne die Einwilligung der betroffenen Kunden ist das datenschutzrechtliche Risiko höher. Was es dann im Rahmen des sog. Pixelverfahrens zu beachten gibt, haben wir für unsere Mandanten bereits in einem früheren Beitrag zusammengetragen.

Die IT-Recht Kanzlei stellt ihren Mandanten zu diesem Thema zudem auch weitere Informationen, etwa auch die entsprechenden Datenschutzerklärungen zur Verfügung. Buchen Sie gerne noch heute eines unserer Schutzpakete!.

Autor:
**RA Dr. Daniel S. Huber**
Rechtsanwalt