von **Dr. Bea Brünen**

Facebook Custom Audience: Vereinbar mit Datenschutzrecht?

Bereits im Jahr 2016 hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) stichprobenartig mehrere Unternehmen hinsichtlich ihrer Verwendung von Facebook Custom Audience überprüft. Im Mittelpunkt standen dabei Facebook Custom Audience über die Kundenliste und das Pixel-Verfahren. Auch in diesem Jahr bleiben die umstrittenen Marketing-Tools im Fokus der Datenschützer. Uns liegt nun ein Schreiben vor, in dem sich das BayLDA zur rechtlich zulässigen Nutzung beider Dienste positioniert. Im Folgenden zeigen wir Ihnen, wie das BayLDA die Facebook-Tools datenschutzrechtlich einordnet und wie eine rechtskonforme Nutzung möglich ist.

A. Rechtliche Fallstricke bei Facebook Custom Audiences

Bei einer Custom Audience handelt es sich um ein Marketing-Tool, mit dem unnötige Werbekosten durch Streuverluste erheblich gesenkt werden können. Ein werbetreibendes Unternehmen kann durch die Definition einer Zielgruppe in seinem Facebook-Account gezielt nur solche Facebook-Nutzer bewerben lassen, bei denen ein Interesse an der jeweiligen Werbung vermutet wird.

Zahlreiche Plattformen bieten Custom Audiences an, wie z. B. Twitter („Tailored Audiences“) und Google („Customer Match Audiences“). Seit Einführung des Marketing-Tools bei Facebook im Jahr 2012 steht jedoch der Zuckerberg-Konzern im Fokus der Datenschützer.

B. Facebook Custom Audience über die Kundenliste

Eine Variante der von Facebook angebotenen zielgruppenorientierten Werbung – und im Fokus der stichprobenartigen Überprüfung des BayLDa – ist Facebook Custom Audience über die Kundenliste. Dieses Tool ermöglicht ein sehr genaues Targeting.

I. Wie funktioniert Custom Audiences über die Kundenliste?

Custom Audience über eine Kundenliste funktioniert folgendermaßen:

1. Schritt:

Das werbetreibende Unternehmen lädt eine eigene Kundenliste mit Daten (z. B. E-Mail-Adresse oder Telefonnummer) von Kunden, die später beworben werden sollen, als Identifikationskennung bei Facebook hoch. Diese Daten werden nicht im Klartext an Facebook versendet, sondern zunächst im Browser mittels SHA256-Verfahrens (Secure Hash Algorithm 256) gehasht und dann verschlüsselt an Facebook übermittelt.

2. Schritt:

Facebook vergleicht die Hashwerte der Kundenliste mit den Hashwerten bereits vorrätiger eigener Nutzerdaten. Durch den Abgleich erfährt Facebook, welcher der Betroffenen zugleich auch Facebook-Nutzer ist.

3. Schritt:

Die Übereinstimmungen werden zu einer Custom Audience auf Facebook zusammengefasst und im Kundenaccount des Werbenden als „Custom Audience“ gespeichert.

4. Schritt:

Das Unternehmen kann nun gezielt Werbung schalten, die nur dem zugeschnittenen Zielpublikum (Custom Audience) angezeigt wird.

II. Die datenschutzrechtliche Problematik von Custom Audiences

Die Problematik hinter Custom Audiences: Die Übermittlung personenbezogener Daten ist nur zulässig, wenn der Betroffene eingewilligt hat oder eine Rechtsgrundlage dafür besteht (§ 4 BDSG). Da eine rechtliche Grundlage für die Übermittlung der Daten nicht besteht, ist das BayLDA der Auffassung, dass Unternehmen vor Übermittlung der Informationen an Facebook eine ausdrückliche Einwilligung des betroffenen Kunden einholen müssen. Dabei stellt sich zunächst jedoch die Frage, ob die übermittelten Daten trotz Verschlüsselung personenbezogene Daten darstellen.

1. Personenbezogene Daten

Bei personenbezogenen Daten handelt es sich um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 Bundesdatenschutzgesetz (BDSG)). Wann genau Daten im Einzelfall als personenbezogen gelten, ist aufgrund dieser doch recht schwammigen Definition nicht immer eindeutig. Man kann sich jedoch merken, dass alle Informationen, über die irgendwie ein Personenbezug hergestellt werden kann, auch unter den Begriff der personenbezogenen Daten fallen. Folgende Daten sind daher unstreitig personenbezogen im Sinne des § 3 Abs. 1 BDSG:

- Name und Anschrift,
- E-Mail-Adresse und Telefonnummer.

Gibt also ein Unternehmen E-Mail-Adressen und Telefonnummern über die Kundenliste an Facebook weiter, übermittelt es personenbezogene Daten i. S. d. § 3 Abs. 1 BDSG.

2. Anonymisierung durch Hashing?

Die personenbezogenen Daten werden jedoch nicht im Klartext an Facebook übermittelt, sondern vorher mittels des SHA-265-Verfahrens gehasht und verschlüsselt an Facebook weiter gegeben. Fraglich ist, ob dadurch eine Anonymisierung der personenbezogenen Daten dergestalt erfolgt, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (§ 3 Abs. 6 BDSG).

Das BayLDA ist der Auffassung, dass das SHA-265-Verfahren kein geeignetes Anonymisierungsverfahren darstellt, da weiterhin ein Rückschluss auf einen konkreten Nutzer von Facebook möglich ist. Das BayLDA argumentiert, dass Facebook „durch einen Vergleich
der Hashwerte feststellen“ kann, „welcher Facebook-Nutzer auch Kunde der verantwortlichen Stelle ist. Dies ist immer dann der Fall, wenn zwei Hashwerte (ein übermittelter und ein von Facebook selbst berechneter) gleich sind. Da zu einem Facebook-Nutzer immer eine E-Mail-Adresse gehört, kann Facebook Ireland Limited dem Hashwert eine E-Mail-Adresse zuordnen, sofern der Inhaber der E-Mail-Adresse auch Facebook-Nutzer ist“.

Mit anderen Worten: Facebook verschlüsselt die E-Mail-Adressen der Facebook-Nutzer nach demselben Verfahren, mit dem es die übermittelten E-Mail-Adressen beim Custom Audience verschlüsselt. Durch einen Vergleich der Hashwerte kann Facebook kinderleicht feststellen, welcher Facebook-Nutzer auch Kunde des jeweiligen Shops ist. Es lässt sich also trotz Verschlüsselung ein Personenbezug herstellen, sodass die Daten von Kunden, die bei Facebook angemeldet sind, für Facebook nicht anonym sind.

Das BayLDA ist zudem der Auffassung, dass der Hashwert der E-Mail-Adresse ohne verhältnismäßig hohen Aufwand mittels der sog. Brut-Force-Methode zurückgerechnet werden kann: „Mithilfe des Verfahrens werden für eine Liste von Klartexten (z. B. E-Mail-Adresse) die dazu gehörenden Hashwerte berechnet. Wird der berechnete Hashwert mit einem vorhandenen Hashwert verglichen und sind beide Hashwerte gleich, ist der passende Klartext (z.B. E-Mail-Adresse) zu dem Hashwert bekannt. Durch diese Methode können viele Hashwerte in den Klartext „zurückberechnet“ werden.“

III. Wie kann man Custom Audiences datenschutzrechtlich sicher nutzen?

Im Datenschutz gilt das sogenannte „Verbot mit Erlaubnisvorbehalt“ (§ 4 Abs. 1 BDSG, § 12 Abs. 1 TMG). Erlaubt ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten danach nur, wenn

- und soweit das BDSG dies erlaubt,
- eine spezielle gesetzliche Regelung dies erlaubt,
- der Betroffene freiwillig und gemäß § 13 Abs. 2 TMG bewusst und eindeutig in die Datenverarbeitung eingewilligt hat.

1. Rechtsvorschrift erlaubt Datenübermittlung

Nach § 28 Abs. 3 Satz 2 Nr. 1 BDSG ist die Übermittlung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ohne Einwilligung zulässig, wenn die in der Norm explizit erwähnten Listendaten, wie Daten über Angehörige einer Personengruppe, Berufs-, Branchen- oder Geschäftsbezeichnungen, Namen, Titel, akademischen Grad, Anschriften oder Geburtsjahr verwendet werden (sogenannte „privilegierte Datenarten“). E-Mail-Adressen gehören jedoch nicht zu den privilegierten Datenarten. Zwar können für Zwecke der Werbung für eigene Angebote § 28 Abs. 3 Satz 2 Nr. 1 BDSG weitere Daten zu den genannten Daten hinzugespeichert werden, jedoch nur, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen (§ 28 Abs. 3 Satz 6 BDSG).

In diesem Fall überwiegen jedoch die Interessen der Betroffenen das Interesse des Shops an personalisierter Werbung. Das BayLDA argumentiert dabei insbesondere mit der mangelnden Erkennbarkeit der Datennutzung. So erhält Facebook durch die Übermittlung der Daten die Information über den Facebook-Nutzer, dass dieser Kunde beim jeweiligen Unternehmen ist. Dieses Wissen nutzt Facebook für eigene Zwecke, indem das bereits vorhandene Profil mit weiteren Merkmalen angereichert wird. Für Kunden bzw. Nutzer ist dies nicht erkennbar. Hinzu kommt, dass die Facebook-Nutzer die Daten, die nun für die personalisierte Werbung eingesetzt werden, nicht zu diesem Zweck preisgeben. Die für die Auswahl der Zielgruppen relevanten Informationen fallen vielmehr im Rahmen der ordentlichen Nutzung von Facebook als soziales Netzwerk an.

2. Einwilligung

Der Einsatz von Custom Audience über die Kundenliste kann demnach nur auf Grundlage einer informierten Einwilligung des Kunden erfolgen. Diese Position vertritt auch das BayLDA. Ohne eine entsprechende Einwilligung ist der Einsatz des Marketing-Tools datenschutzrechtlich unzulässig.

a. Rechtliche Anforderungen an eine wirksame Einwilligung

Eine wirksame elektronische Einwilligungserklärung setzt voraus, dass

- der Kunde seine Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung protokolliert wird,
- der Kunde den Inhalt der Einwilligung jederzeit abrufen kann und
- der Kunde die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

Zudem ist der Kunde im Rahmen der Einwilligung konkret und verständlich über die Datennutzungsvorgänge zu informieren, für die er seine Zustimmung erteilt. Diese sind möglichst genau zu bestimmen und müssen dem Kunden eine informierte Entscheidung ermöglichen, seine Einwilligung im konkreten Fall zu erteilen oder zu versagen. Über die im Rahmen der Einwilligungserklärung aufgeführten Zwecke und Prozesse darf der Seitenbetreiber nicht hinausgehen, d. h. die Daten dürfen nur in dem Maße verwendet werden, wie sie von den in der Einwilligung ausgewiesenen Nutzungsvorgängen gedeckt sind.

b. Umsetzung der Anforderungen

Um die Datenübermittlung zu legitimieren, müssen diese Anforderungen vom Shop-Betreiber vollumfänglich eingehalten werden. Welche Umsetzungsmaßnahmen konkret erforderlich sind, zeigen wir im Folgenden.

aa. Opt-in oder Opt-out?

Der Kunde muss seine Einwilligung bewusst und eindeutig erteilt haben. Ein Dauerbrenner im Datenschutzrecht und von der Rechtsprechung bislang nicht abschließend geklärt ist dabei, ob dieser Anforderung nur durch eine aktive Einwilligungshandlung („Opt-in“) entsprochen wird, oder ob die Vorformulierung der Einwilligungserklärung seitens des Webseitenbetreibers und die grundsätzliche Widerspruchsmöglichkeit des Kunden („Opt-out“) genügt. So wird es teilweise für erforderlich gehalten, dass der Einwilligende mittels „Opt-In“, also durch Setzen eines Häkchens neben einem vorgefassten Einwilligungstext, seine Erklärung erteilt. Teilweise wird es aber auch als ausreichend empfunden, die Einwilligungserklärung ohne besondere Möglichkeit der Akzeptanz dem Feld beizustellen, durch dessen Anklicken die Daten übermittelt werden. Auch das BayLDA äußert sich nicht ausdrücklich dazu, welches Verfahren es im Rahmen der Nutzung der Custom Audience über die Kundenliste für notwendig erachtet.

Auf der vollständig rechtssicheren Seite bewegt sich der Seitenbetreiber aber, wenn er die Einwilligungserklärung tatsächlich mit einer „Check-In-Box“ versieht und ein Absenden des Formulars vom Setzen eines entsprechenden Häkchens abhängig macht. Dies führt dem Nutzer nämlich in besonders prägnanter Weise die Rechtserheblichkeit seiner Einwilligung vor Augen und stellt sicher, dass er in die Übermittlung der Daten im Bewusstsein der Tragweite einwilligt.

Die IT-Recht-Kanzlei empfiehlt insofern eine Einwilligungseinholung per „Opt-In-Box“, die sinnvollerweise in den Bestellprozess beim Check-Out implementiert werden sollte.

bb. Oberstes Gebot: Transparenz

Die Einwilligung sollte Antworten auf folgende Fragen geben:

- Welche Daten werden erhoben?
- Zu welchen Zwecken werden die Daten verwendet?
- Wie lange werden die Daten aufbewahrt?

Der Kunde muss wissen, was auf ihn zukommt, wenn er dem Shop eine Einwilligung in die Übermittlung seiner Daten an Facebook erteilt. Die bereitzustellende Einwilligungserklärung muss genau ausweisen, unter und zu welchen Bedingungen welche Daten genutzt werden dürfen. Dazu gehört auch, dass das Unternehmen Facebook als Datenempfänger benennt und den Betroffenen darüber aufklärt, wie die Daten bei Facebook ausgewertet werden. Zudem ist darauf hinzuweisen, dass die erteilte Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden kann.

cc. Dokumentation der Einwilligung

Eine wirksame Einwilligung sollte zudem beweisbar sein. Dies setzt voraus, dass der Shop Vorkehrungen trifft, damit das Vorliegen einer Einwilligung jederzeit nachgewiesen werden kann. Dazu sollten die IP-Adresse, der Timestamp, der dazugehörige Einwilligungstext sowie die anschließende Bestätigung der Einwilligung – in ausdruckbarer Form – abgespeichert werden.

dd. Ergänzender Hinweis in der Datenschutzerklärung

Aus Gründen der Rechtssicherheit und der von § 13 Abs. 3 Satz 2 i. V. m. Abs. 1 Satz 3 TMG geforderten „ständigen Abrufbarkeit“ sollte der Hinweis auf die Widerrufsmöglichkeit der Einwilligung unter einer eigenen Überschrift (bspw. „Nutzung von Re-targeting Tools“) in die nach § 13 Abs. 1 TMG verpflichtende Datenschutzerklärung aufgenommen werden. Innerhalb des Passus kann zudem erneut über die Einsatzbestimmung der übermittelten personenbezogenen Daten informiert werden. Sinnvollerweise sollte in der Datenschutzerklärung zudem auf die von Facebook bereitgestellten, ergänzenden Informationen sowie auf die Möglichkeit, dem Targeting bei Facebook zu widersprechen, hingewiesen werden (https://www.facebook.com/ads/website_custom_audiences/). Sinnvoll ist es zudem, auf das Auskunftsrecht des § 19 BDSG gesondert hinzuweisen.

C. Facebook Custom Audience Pixel-Verfahren

Eine weitere Variante der zielgruppenorientierten Werbung ist das sogenannte Pixel-Verfahren, das auch als „Facebook Custom Audience from Website“ bezeichnet wird.

I. Wie funktioniert das Facebook Custom Audience Pixel-Verfahren?

Beim Pixel-Verfahren bindet ein Seiteninhaber einen unsichtbaren Pixel als Code auf der Webseite ein, welches Wiederkehrer erkennt und ein Nutzungsprofil auf (vermutlich) pseudonymer Basis erstellt. Facebook erkennt so, welche User die Website besucht haben und zeigt nur ihnen Werbung des Webseiten-Inhabers an.

II. Die datenschutzrechtliche Problematik

Das BayLDA hält den Einsatz des Pixel-Verfahrens auf Grundlage von § 15 Abs. 3 TMG für zulässig. Diese Vorschrift erlaubt die Verwendung pseudonymer Nutzungsprofile zu Werbezwecken.

III. Wie kann man das Facebook Custom Audience Pixel-Verfahren datenschutzrechtlich sicher nutzen?

Die Vorgaben für die rechtliche Zulässigkeit des Pixel-Verfahrens richten sich somit nach § 15 Abs. 3 TMG. Danach darf der Diensteanbieter für Zwecke der Werbung Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Erforderlich ist demnach, dass der Kunde der Nutzung seiner Daten widersprechen kann. Das bedeutet: Gibt es keine Opt-Out-Möglichkeit in der Datenschutzerklärung, ist der Einsatz des Pixel-Verfahrens unzulässig. Darüber hinaus sollte auch hier die Datenschutzerklärung ergänzt und umfangreich über den Einsatz des Pixel-Verfahrens informiert werden (s. o. „Ergänzender Hinweis in der Datenschutzerklärung“).

D. Empfehlung

Die Anschreiben des BayLDA dienen voraussichtlich der Einleitung von Bußgeldverfahren, bei denen sich die Höhe der Bußgelder nach der Anzahl der rechtswidrig hochgeladenen Daten bemisst. Um Bußgelder zu vermeiden, sollten Unternehmen, die die Marketing-Tools von Facebook nutzen möchten, die Rechtsansicht des BayLDA berücksichtigen und ihre Website sowie die Datenschutzerklärung dementsprechend anpassen.

Autor:
Dr. Bea Brünen
(freie jur. Mitarbeiterin der IT-Recht Kanzlei)