KURZDARSTELLUNG

SO BRINGEN SIE

PERSONALISIERUNG, DATENSCHUTZ UND EINE OPTIMALE BENUTZERERFAHRUNG

UNTER EINEN HUT

Ping Identity

KUNDEN ERWARTEN INTERAKTIONEN AUF BASIS VON PERSONALISIERUNG UND DATENSCHUTZ

Digitale Geschäftsmodelle bieten interessante Möglichkeiten, um jederzeit und überall mit Kunden zu interagieren. Mobilgeräte, das Internet der Dinge (Internet of Things, IoT) und andere Interaktionskanäle eröffnen neue Chancen, um Daten für die Personalisierung der Kundenerfahrung zu sammeln. Egal, wo Ihre Kunden auf Ihre Marke treffen – Sie sollten immer darauf vorbereitet sein, ihnen eine nahtlose, sichere und interaktive Erfahrung zu bieten.

Doch Kunden machen sich Gedanken darüber, wie Unternehmen ihre Informationen nutzen und weitergeben, und sind immer weniger bereit, mehr als nur die unbedingt notwendigen Daten preiszugeben. Eine vor kurzem durchgeführte Umfrage ergab, dass 71 Prozent der Verbraucher der Meinung waren, dass Unternehmen, die Zugriff auf ihre persönlichen Daten haben, diese auf unethische Weise nutzen.[1] Die gleiche Umfrage zeigte auch, dass über die Hälfte keine Onlineservices nutzt, weil sie sich um den Datenschutz sorgt.

Diese Sorge der Kunden sowie der Flickenteppich aus neuen regionalen Regelungen, Branchenvorgaben und Firmenrichtlinien zum Datenschutz zwingen Organisationen, die Privatsphäre ihrer Kunden zu schützen und bei der Erfassung und Weitergabe von Kundendaten besonders vorsichtig zu sein. Trotz der komplizierten Situation müssen Unternehmen Daten sammeln, um die interaktive und personalisierte Erfahrung zu bieten, die Kunden heute erwarten.

Diese widersprüchlichen Anforderungen zu erfüllen ist nicht so aussichtslos, wie es auf den ersten Blick erscheinen mag. Speziell entwickelte Customer-Identity- und Access-Management(CIAM)-Plattformen bieten die nötigen Funktionen, um beiden Ansprüchen gerecht zu werden. Mit der richtigen Lösung können Unternehmen die Kundeneinwilligung zur Datenweitergabe sowie die Einhaltung von Datenschutz-bestimmungen umsetzen und gleichzeitig Präferenzen und andere für die Personalisierung benötigten Kundendaten speichern und verwalten.

Über die Hälfte der Verbraucher gibt an, keine Onlineservices zu nutzen, weil sie sich Sorgen um den Datenschutz macht.[2]

UNTERNEHMEN MÜSSEN DAS RICHTIGE VERHÄLTNIS ZWISCHEN PERSONALISIERUNG UND DATENSCHUTZ FINDEN

Wenn Kunden der Ansicht sind, dass ein Unternehmen verantwortungsvoll mit ihren Daten umgeht, bleiben sie der Marke treu und empfehlen sie weiter. Organisationen hingegen, die es nicht schaffen, ihre Daten vor unautorisierter Weitergabe, Lecks und Missbrauch zu schützen, verlieren schnell das Vertrauen der Kunden und müssen Umsatzeinbußen hinnehmen.

> „Der Umgang einer Organisation mit privaten Kundendaten entwickelt sich zunehmend zu einem Differenzierungsmerkmal."[3]
>
> -Forrester

Die Sorge um den Datenschutz führt auch zu immer strengeren und komplexeren Datenschutzvorgaben. Gesetzliche Vorgaben können für bestimmte Regionen, Branchen und sogar für demographische Gruppen angewendet werden. In Europa schreibt die Datenschutz-Grundverordnung (DSGVO) vor, wo die Daten europäischer Bürger zu speichern, wie Kundeneinwilligungen umzusetzen und auf welche Weise Daten zu erfassen sind. Nach Inkrafttreten der neuen Verordnung im Mai 2018 drohen Organisationen bei Nichteinhaltung Geldstrafen von bis zu vier Prozent ihres Jahresumsatzes oder zehn Millionen Euro.

Um in diesem zunehmend komplexen Umfeld zu bestehen, müssen Organisationen sorgfältig prüfen, welche Attribute ihrer Kundendaten sie Anwendungen zugänglich machen. Sie müssen dafür sorgen, dass Apps nur auf die erforderlichen Attribute zugreifen und insbesondere bei Partneranwendungen sicherstellen, dass Kunden in die Weitergabe ihrer Daten eingewilligt haben. Darüber hinaus müssen sie die Einwilligungsprozesse intuitiv gestalten. Ellenlange Datenschutzrichtlinien in juristischen Schachtelsätzen gehen heute nicht mehr. Stattdessen erwartet der Kunde benutzerfreundliche Kontrollmöglichkeiten, mit denen er seine Einwilligungen managen und klar sehen kann, wer Zugriff auf seine Daten hat.

Zentralisierte Funktionen für das Datenschutzmanagement ermöglichen es, die wachsende Anzahl dynamischer Datenschutzbestimmungen einzuhalten. Mit zentralisierten Regeln können Sie kontrollieren, wie und wo Daten eingesetzt werden. Ohne solche Regeln ist es riskant, neue Initiativen zur Verbesserung der Kundenerfahrung einzuführen, und es kann passieren, dass die Sicherheits-, Legal- und Compliance-Teams die Datennutzung stark eingrenzen. In einer modernen Multichannel-Umgebung, in der Wettbewerbsvorteile von der Personalisierung abhängen, wäre das ein großer Nachteil.

Aber wie können Organisation Kundendaten einsetzen, um eine personalisierte Erfahrung bereitzustellen?

Lassen Sie zuerst Ihre Kunden ihre Präferenzen explizit nennen. Wenn Sie sich auf implizite Präferenzen aus dem Browserverlauf oder von Marketingplattformen verlassen, kann das zu ungenauen Annahmen führen.

Verwenden Sie anschließend ein sicheres, zentralisiertes Repository, um Kundendaten und Präferenzen aus unterschiedlichen Anwendungen und Kanälen zu speichern und zu verwalten. Sorgen Sie dafür, dass ausreichend Kapazitäten für Kundenanwendungen vorhanden sind, und dass sich Kundendaten über entwicklerfreundliche REST APIs ausgeben lassen.

PRÄFERENZ- UND DATENSCHUTZMANAGEMENT IN DREI SCHRITTEN

In digitalen Unternehmen spielen Personalisierungs- und Datenschutzmanagement eine entscheidende Rolle, um gesetzliche Vorgaben einzuhalten und eine nahtlose und sichere Kundenerfahrung zu schaffen. Achten Sie bei der Evaluierung einer CIAM-Plattform darauf, dass die Lösung die folgenden Features bietet:

01 Einheitliches Kundenprofil

Digitale Unternehmen erzeugen und nutzen Daten über mehrere Kundenkontaktpunkte, Geräte und Apps sowie interne Geschäftseinheiten und externe Partner hinweg. Ein effektives Personalisierungs- und Datenschutzmanagement erfordert die Speicherung von Kundenpräferenzen, Einwilligungsentscheidungen und anderen Daten in einem sicheren, skalierbaren einheitlichen Profil, das für alle Anwendungen zugänglich ist. Eine umfassende Sicht auf den Kunden schließt viele verschiedene Datentypen mit ein, einschließlich strukturierter Informationen wie Name, Alter und Kontaktdaten, sowie unstrukturierter Daten wie Kaufhistorie und Verhaltensmuster. CIAM-Plattformen unterstützen Sie dabei, alle Ihre bestehenden Daten in ein einheitliches Kundenprofil zu migrieren oder zu synchronisieren. Anschließend können Sie alle Kundendaten einschließlich impliziter und expliziter Präferenzdaten verwalten. Auf diese Weise schaffen Sie äußerst wertvolle Profile, die präzise Informationen darüber bieten, wer der Kunde ist und was er möchte.

02 Regelbasierte Data-Governance

Der Schutz privater Kundendaten und die Einhaltung von Vorgaben sind komplexe Aufgaben. Oft ist dazu die Durchsetzung und Kontrolle von Regeln auf mehreren Ebenen notwendig. Achten Sie darauf, dass Ihre Lösung regelbasierte Data-Governance-Funktionen bietet, mit denen Sie regionale, unternehmens- oder branchenspezifische Richtlinien einhalten und Kundeneinwilligungen umsetzen können. Außerdem sollte Ihre CIAM-Plattform mehr tun, als nur den Zugriff auf ein Kundenprofil als Ganzes zu verwalten: Sie sollte in fein abgestufter Form darüber entscheiden können, auf welche Datenattribute innerhalb des Profils zugegriffen werden kann. Zum Beispiel benötigt ein externer E-Mail-Marketing-Partner in der Regel Zugriff auf Kundennamen, E-Mail-Adressen und Opt-in-Präferenzen, jedoch nicht auf Zahlungsinformationen. Möglicherweise möchten Ihre Kunden auch, dass bestimmte Attribute wie z. B. ihre E-Mail-Adressen nicht an bestimmte Partneranwendungen weitergegeben werden. Im digitalen Ökosystem sind die Weitergabe von Daten an externe Serviceprovider sowie Data-Brokering immer geläufiger. Regelbasierte Data-Governance sorgt dafür, dass Sie alle geltenden Regelungen einhalten und Ihre Kunden erfahren und kontrollieren können, wohin ihre Daten gehen.

03 Einwilligungsmanagement

Kunden erwarten eine positive, benutzerfreundliche Erfahrung, wenn sie mit Ihrer Marke interagieren, und möchten ihre Datenschutzeinwilligungen selbst verwalten können. Mit einem zentralisierten Profil zur Speicherung von Datenschutzeinstellungen und Einwilligungspräferenzen, die wiederum mit zentralisierten Regeln umgesetzt werden, können Sie Ihren Kunden die eigenen Daten auf sämtlichen Kanälen bereitstellen. Sie können dazu intuitive Kontrollen nutzen, mit denen Ihre Kunden einsehen können, wer Zugriff auf ihre Daten hat, und entscheiden, welche Attribute sie teilen wollen. Dieser Ansatz ist um einiges besser, als Kunden in ellenlangen Datenschutzrichtlinien, die alle Eventualitäten abdecken, um ihre Einwilligung zu bitten. Wenn Sie sich die Zeit nehmen, Ihren Kunden diese Informationen und Kontrollmöglichkeiten bereitzustellen, vermitteln Sie ihnen das Gefühl, dass ihre Daten in guten Händen sind.

FAZIT

Laut Forrester sind Marketingabteilungen immer häufiger gezwungen, sich mit dem Datenschutz auseinanderzusetzen. Zurückzuführen ist dies auf moderne Digital-Business-Praktiken, insbesondere dem Behavioral Targeting, dem standortbasierten mobilen Marketing und der Schaffung einer durchgängigen Multichannel-Kundenerfahrung.[4] Digitale Technologien bieten zwar immer mehr Möglichkeiten, mit Kunden zu interagieren, doch müssen Unternehmen vorsichtig sein, keine Grenzen zu überschreiten, die in Richtung negative Kundenerfahrung gehen könnten. CIAM-Lösungen bieten effiziente Personalisierungs- und Datenschutzmanagement-Funktionen, mit denen sich der schmale Grat zwischen der Einhaltung von Datenschutzrichtlinien und der effizienten Nutzung von Kundendaten zu Personalisierungszwecken meistern lässt.

1. *Mindi Chahal, „Marketers Overestimate Consumers' Attitude to Data" (Marketingexperten unterschätzen die Sorgen der Verbraucher um ihre persönlichen Daten), Marketing Week, 23. Juni 2016, abgerufen am 17. Juli 2017 unter https://www.marketingweek.com/2016/06/23/marketers-overestimate-consumers-attitude-to-data/*
2. *Ibid.*
3. *Vendor Landscape: Privacy-Support Providers for Marketers (Anbieter im Bereich Datenschutz für Marketingexperten), The Customer Trust And Privacy Playbook For 2017 (Playbook 2017 zu Kundenvertrauen und Datenschutz), Forrester Research, letztes Update 25. August 2016.*
4. *Ibid.*

#3164 | v00d | 07.17