



Die Rolle der CDP in stark regulierten Branchen: Banking



Inhalt

Vorwort	3
Der springende Punkt: Anonymisierung und Pseudonymisierung	4
Die Rolle der CDP im Banking	6
Governance und Folgen	10
Abschließendes Fazit	12



Vorwort

Niemand kennt uns so gut wie unsere Bank. Sie weiß fast mehr über uns als wir selbst – oder zumindest mehr als wir uns eingestehen wollen.

Banken wissen jeden Tag auf den Cent genau, wofür, wann, für welche Marken und wie wir unser hart verdientes Geld ausgeben. Sie kennen unser Lieblingscafé und den Favoriten unter unseren Lieferdiensten. Wohin es in Urlaub geht, erfahren sie ebenfalls. Und sie wissen nicht nur, wann wir heiraten, sondern auch, wann wir eine Familie gründen.

Alles in unserem Leben hängt mit unseren Finanzen zusammen. Deshalb ist auch unser Verhältnis zu der Bank, die unser Geld verwaltet, ausgesprochen wichtig. Dabei hat sich im Zuge technologischer Entwicklungen die Art und Weise, wie wir mit unseren Banken interagieren, verändert – überwiegend zum Positiven. Ich bin alt genug, um mich noch daran zu erinnern, wie ich mit meinem Sparbuch in der Bank Schlange stand, um Bargeld abzuheben. Und hatte man die Öffnungszeit verpasst, war's das. Dann hatte man eben kein Geld.

Andererseits gab es dort immer Mitarbeitende, die einen kannten und die Macht hatten, Entscheidungen zu treffen – das Zeitalter des „Computer sagt Nein“ lag noch weit in der Zukunft.

Im Zeitalter des technologischen Fortschritts hingegen stehen Banken unter Druck. Es wird erwartet, dass sie sich schnell auf die Forderungen und Erwartungen der Verbraucher einstellen. Banken müssen mehr sein als nur eine Alternative zum Gelddepot unter der Matratze.

Die Vielfalt an Plattformen geht jedoch mit neuen Herausforderungen in Bezug auf regulatorische Aspekte und Haftung einher. Die zunehmende Benutzerfreundlichkeit auf Mobilgeräten, Desktops und Tablets führt zu mehr potenziellen Schwachstellen, da jede neue App und Schnittstelle ein zusätzliches Risiko darstellt.

Diese Tatsache darf jedoch keinesfalls Innovationen im Weg stehen. Vielmehr muss die Branche Kundendaten intelligenter nutzen, zugunsten von mehr Kundentreue und besseren Experiences.

Das ist nicht ganz einfach. Aber zum Glück machbar.

Lindsay McEwan

Senior Vice President, EMEA GM, Tealium

Der springende Punkt: Anonymisierung und Pseudonymisierung

Bevor wir darüber sprechen, welche Rolle eine CDP in einer stark regulierten Branche spielen kann, befassen wir uns zunächst mit den beiden zentralen Aspekten des Datenmanagements, die über den Erfolg einer CDP entscheiden: Anonymisierung und Pseudonymisierung.

Sie zu verstehen ist wesentlich, um DSGVO-Compliance und Daten-Insights miteinander in Einklang zu bringen.

Anonymisierung

Darunter versteht man den Ausschluss jeglicher Möglichkeit, einen bestimmten Kunden zu identifizieren. Die vorhandenen Daten werden vollkommen von ihrem Inhaber losgelöst und können daher nur als absolute Werte betrachtet werden. Anonymisierte Daten zeigen zum Beispiel, wie viele Bankkunden ihr Portfolio über das Girokonto hinaus mit Sparanlagen und Sparplänen erweitert haben.

Auf diese Weise zeigen die Daten Makrotrends über die gesamten Kundendatensätze hinweg auf. Aber für eine Bank ist es damit nicht möglich festzustellen, wer zusätzlich zu seinem Girokonto einen Sparplan eingerichtet hat und welche anderen Produkte oder Dienstleistungen für diese Person interessant sein könnten. Die Anonymisierung kann Informationen für die Geschäftsstrategie beisteuern und darüber, wo Marketingmaßnahmen greifen könnten, aber nur aus einer Top-Down-Perspektive.



Pseudonymisierung

Ausschließlich anonymisierte Daten zu verwenden, beseitigt zwar sämtliche Risiken im Umgang mit Kundendaten, bietet jedoch, wie bereits erwähnt, keine Transparenz und liefert nicht wirklich Informationen, die man für spezifische Maßnahmen auf der Grundlage von Insights nutzen könnte.

Mit einer pseudonymisierten Ebene im Datenmanagement hingegen können Unternehmen ihren Marketing-Output personalisieren und gleichzeitig die DSGVO einhalten sowie Kundendaten schützen.

Dafür werden die einzelnen Kundendatenpunkte vor der Analyse mit Tags versehen – aus „Florian Müller“ wird beispielsweise „BankKunde001“. Innerhalb der CDP lassen sich Pseudonyme jedoch sicher entschlüsseln, um die jeweilige Person und ihre Kontaktdaten zu ermitteln, damit die Bank auf die jeweiligen Kunden zugehen kann.

Marketing mit Identifiern

Die Bank erhält also Verhaltensdaten über BankKunde001 – Vorlieben, Abneigungen, Cashflow, bevorzugte Geschäfte, Cafés und Urlaubsorte.

Entscheidend dabei ist, dass die Bank nur weiß, was ein bestimmter Identifier tut. Sie weiß nicht unmittelbar, dass es sich dabei um Florian Müller handelt. Aufgrund der Pseudonymisierung der Daten hält die Bank die DSGVO-Bestimmungen ein und schöpft gleichzeitig die Daten aus, die sie besitzt.

Der Vorteil: BankKunde001 wird zu einem Marketing-Stapel hinzugefügt und erhält bestimmte Werbeaktionen und Angebote – die alle relevant sind und gleichzeitig im Einklang mit dem Datenschutz stehen. Und somit steht es den Banken frei, bestimmte Insights mit Dritten und Marken zu teilen und dabei ihre Compliance einzuhalten.



Die Rolle der CDP im Banking

CDPs und Win-Win

Für die Betrachtung, wie eine CDP das Wachstum und die Kundenbindung im Privatkundengeschäft fördern kann, sind zwei voneinander abhängige Aufgabenbereiche zu berücksichtigen.

Erstens muss die CDP natürlich – wie in jeder Kunden zugewandten Branche – einen kommerziellen Zweck erfüllen: Sie muss dafür sorgen, dass die Kunden der Bank möglichst viel Geld auf ihre Konten einzahlen, investieren und im Zuge des Cross-Selling für Versicherungen und andere Produkte ausgeben. Dieselbe Vorgehensweise kann auch auf Marken- und Einzelhandelspartner ausgedehnt werden, die von der Bank gespeicherte Daten für Werbeaktionen nutzen.

Zweitens muss dieser Prozess mit der Unterstützung des Kunden während seiner gesamten Life Journey Hand in Hand gehen. Kunden verändern sich im Lauf der Zeit, und Banken können die Kundenbindung fördern, wenn sie die Customer Journey verstehen und entsprechend reagieren.

Die Kombination aus den beiden genannten Faktoren führt zu einem höheren Lifetime Value: Je besser es der Bank gelingt, lebenslang ein wichtiger Partner zu sein, desto mehr Geld vertrauen Kunden der Bank an.

Treue Kunden teilen Daten

Kunden erwarten nicht nur, dass sie von Marken Werbeaktionen und besondere Angebote erhalten – sie verlangen es. Sie möchten sich verstanden, wertgeschätzt und wichtig fühlen. Das Teilen von Daten erfolgt nach dem Prinzip „quid pro quo“.

Allerdings bieten Privatkundenbanken – insbesondere alteingesessene Großbanken – nicht immer die gewünschte VIP-Behandlung. Angesichts der Daten, die Banken darüber vorliegen, wie und wofür das Geld ihrer Kunden ausgegeben wird, grenzt es an unternehmerische Naivität, sich diese Gelegenheit entgehen lassen.

Da die Finanzdaten von Kunden mit äußerster Sensibilität behandelt werden müssen, könnte man meinen, dass Banken davor zurückschrecken, diese Daten für Werbezwecke zu verwenden.

Tatsächlich jedoch haben unsere Untersuchungen aus dem Jahr 2021 ergeben, dass durchaus ein großes Interesse an auf Kundendaten basierenden Werbeaktionen und Vorteilsangeboten von Bankpartnern besteht.



Verpasste Chancen

Obwohl ihre Zielgruppe sehr aufgeschlossen wäre, nutzen Privatkundenbanken ihre Chance für Werbeaktionen und Vorteilsangebote offensichtlich nicht. Die Umfrage ergab, dass derzeit durchschnittlich drei von zehn europäischen Privatkundenbanken Angebote und Werbeaktionen versenden. Dem gegenüber stehen jedoch zwei Drittel der Kunden, die ihrer Bank vertrauen würden, wenn sie personalisierte Werbeaktionen anbietet.

Tatsächlich vertrauen Verbraucher beim Thema personalisierte Werbung am ehesten ihrer Bank (67 % der Befragten), verglichen mit ihrem Supermarkt vor Ort (57 %), dem Online-Händler, den sie am häufigsten nutzen (54 %), oder ihrem Mobilfunkanbieter (52 %).

Sich dieses Vertrauen nicht zunutze zu machen, bedeutet, ein riesiges Potenzial an Chancen ungenutzt zu lassen. Marken müssen verstehen, welche Gelegenheiten diese Offenheit für Banken als Kanal zu den Verbrauchern mit sich bringt – aber es ist die Aufgabe des Finanzsektors, dieses Wissen zu vermitteln.

Sichere Analyse

Die oben beschriebenen Fakten verdeutlichen, dass eine CDP Banken dabei unterstützen kann, für ihre Kunden unverzichtbar zu werden und potenzieller Abwanderung aktiv entgegenzuwirken.

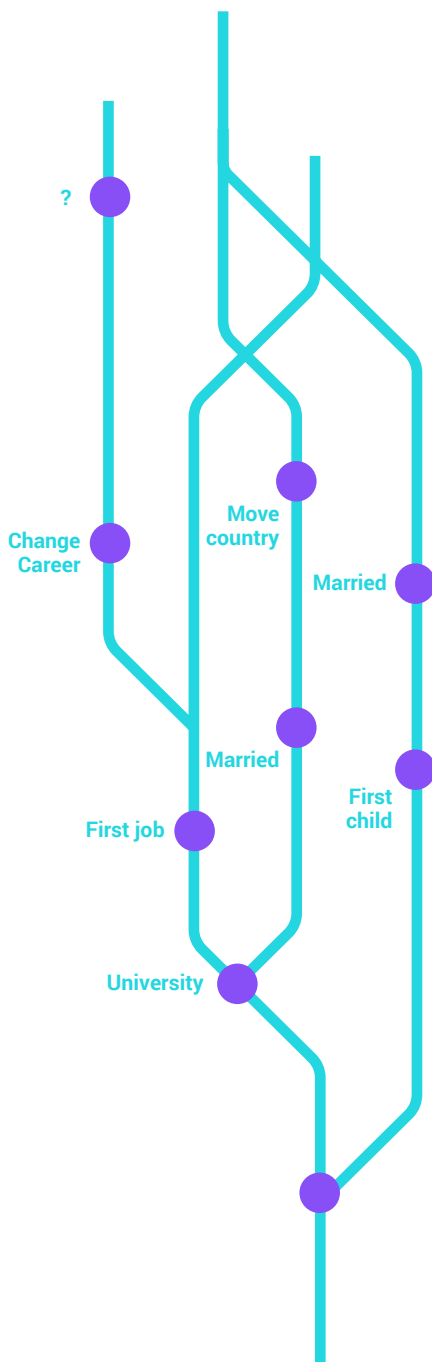
Dank des hohen Sicherheitslevels einer CDP sind Banken dazu in der Lage, Kaufdaten zu analysieren und auf Marken zuzugehen mit dem Wissen, welche (pseudonymisierten) Kunden regelmäßig bei ihnen kaufen. Banken gehen dadurch eine direkte Partnerschaft mit bekannten Käufern ein und werden so ihrerseits zu einem wesentlichen Teil eines Marketing-Ökosystems und zu einer direkt an den Verbraucher gerichteten Werbemaßnahmen.

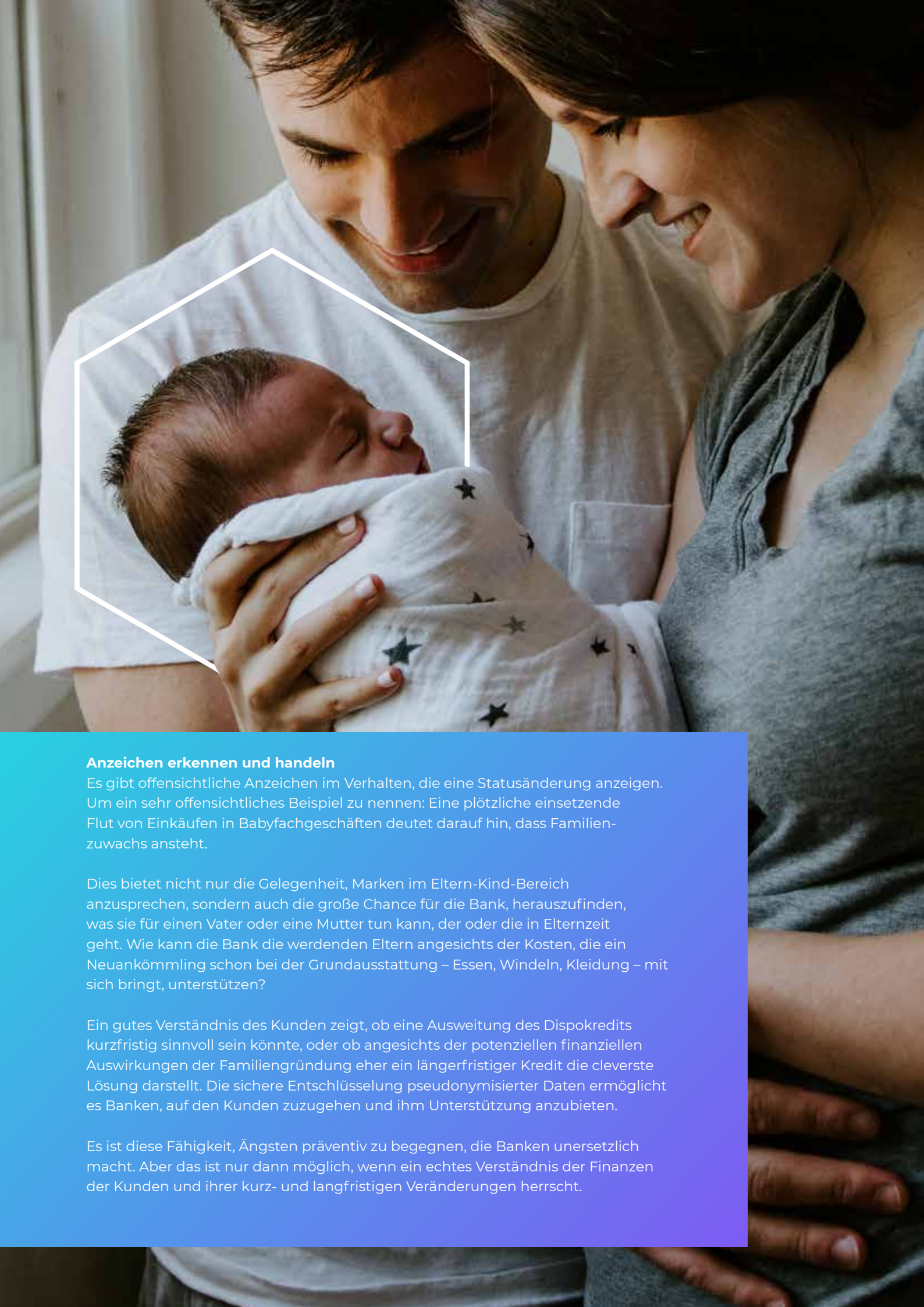
Dennoch könnten regulatorische Aspekte Besorgnis erregen. Datenanalysen einzusetzen, um Daten für Werbemaßnahmen zu liefern und dadurch mit Marken und Partnern Geschäftschancen zu nutzen, bringt neue Compliance-Anforderungen mit sich. Aber die Fähigkeit, Risiken durch eine CDP zu managen, macht die Compliance gleichzeitig zu einem Hygienefaktor innerhalb der Analyse.

Kunden und ihre Life Journey

Bankkunden sind viel mehr als nur eine Kontonummer. Sie sind eine Gruppe von Individuen, die alle ihren eigenen Lebensweg gehen. Kein Leben gleicht dem anderen, und deshalb muss eine Bank nicht nur die Customer Journey, sondern die Life Journey jedes einzelnen Kunden betrachten. Ein herkömmliches Programm zur reinen Markenpflege reicht deshalb nicht aus.

Banken müssen verstehen, wo sich der Kunde auf seiner Reise befindet und was er von seiner Bank gerade braucht. Und auch wenn jeder Weg anders ist, gibt es dennoch viele gemeinsame Meilensteine: Schulabschluss, Partnersuche, Kauf oder Miete einer Immobilie, Kinder, Ruhestand (wenn auch nicht immer in dieser Reihenfolge).





Anzeichen erkennen und handeln

Es gibt offensichtliche Anzeichen im Verhalten, die eine Statusänderung anzeigen. Um ein sehr offensichtliches Beispiel zu nennen: Eine plötzliche einsetzende Flut von Einkäufen in Babyfachgeschäften deutet darauf hin, dass Familienzuwachs ansteht.

Dies bietet nicht nur die Gelegenheit, Marken im Eltern-Kind-Bereich anzusprechen, sondern auch die große Chance für die Bank, herauszufinden, was sie für einen Vater oder eine Mutter tun kann, der oder die in Elternzeit geht. Wie kann die Bank die werdenden Eltern angesichts der Kosten, die ein Neuankömmling schon bei der Grundausstattung – Essen, Windeln, Kleidung – mit sich bringt, unterstützen?

Ein gutes Verständnis des Kunden zeigt, ob eine Ausweitung des Dispokredits kurzfristig sinnvoll sein könnte, oder ob angesichts der potenziellen finanziellen Auswirkungen der Familiengründung eher ein längerfristiger Kredit die cleverste Lösung darstellt. Die sichere Entschlüsselung pseudonymisierter Daten ermöglicht es Banken, auf den Kunden zuzugehen und ihm Unterstützung anzubieten.

Es ist diese Fähigkeit, Ängsten präventiv zu begegnen, die Banken unersetzlich macht. Aber das ist nur dann möglich, wenn ein echtes Verständnis der Finanzen der Kunden und ihrer kurz- und langfristigen Veränderungen herrscht.



Die Entwicklung der Digitalisierung

Wie gut sich Banken während der Life Journey ihrer Kunden als Partner bewähren können, hängt im Wesentlichen von der wachsenden Datenmenge ab, die sie sammeln. Der Datenanstieg ist eine direkte Folge der rasanten Digitalisierung der Branche in den letzten Jahren und der Erwartung der Kunden, mit ihrer Bank über eine Vielzahl von Plattformen in Kontakt treten zu können.

Der Prozess wurde zum Teil durch die explosionsartige Zunahme konkurrierender (meist Digital-First-)Banken im Gegensatz zu Großbanken und ihren physischen Filialen vorangetrieben. Letztere mussten schnell handeln, um mit den digital bestens aufgestellten Onlinebanken Schritt halten zu können, die von Anfang an sehr intuitive Services angeboten haben.

Diese Entwicklung hat dazu geführt, dass Kunden eine nutzerfreundliche Online-Experience erwarten, und zwar über die Benutzeroberflächen von Desktop-, App-, Mobil- und Tablet-Anwendungen hinweg. Nachdem Finanzen ein sensibler Teil des Lebens sind, löst jede Art von Fragmentierung oder fehlender Synchronisierung Alarm aus. Ironischerweise wurden die digitalen Plattformen nicht zu einem positiven Unterscheidungsmerkmal, sondern vielmehr zu einer Quelle der Unzufriedenheit und potenziellen Abwanderung.

Abgesehen von veränderten Verhaltensweisen kamen auf die Banken neue regulatorische Herausforderungen zu. Sie wurden dazu verpflichtet, ihre Kunden anzusprechen und festzustellen, wie sich veränderte Umstände auf ihre Finanzen auswirkten, und gegebenenfalls zu unterstützen.

Die Banken, die über keine voll funktionsfähigen digitalen Systeme verfügten, entdeckten jedoch, in welchem Umfang (nicht-finanzielle) Kundendaten bei Dritten gespeichert waren. Alle Daten im Besitz der Banken waren anonymisiert, so dass sie bei der direkten Kontaktaufnahme auf Informationen aus externen Quellen angewiesen waren, die über Daten ihrer Kunden verfügten.

In diesem Fall bedeutete das „berechtigte Interesse“, dass Banken diese externen Daten als ihre eigenen Pseudo-First-Party-Daten nutzen konnten. Ein solcher Weckruf könnte als glücklicher Umstand gewertet werden. Besser wäre es jedoch, betriebliche Schwachstellen auch ohne radikale Veränderungen aufzudecken.

„Während der Pandemie wurde deutlich, wie weit die Banken auf ihrem eigenen Weg der digitalen Transformation fortgeschritten sind. Schätzungen zufolge hat sich ein früheres Verhältnis von 80:20 zwischen Online- und mobilem Zugang innerhalb weniger Monate zum umgekehrten Wert von 20:80 entwickelt. Mobile Nutzung ist inzwischen nahezu Standard.“



Governance und Folgen

Der Bankensektor ist eine der am stärksten regulierten Branchen der Welt – aus naheliegenden Gründen. Aufsichtsbehörden stellen nicht nur sicher, dass Daten und Kundeninformationen sicher aufbewahrt werden (bei Verstößen drohen hohe Geldstrafen und Lizenzentzug), sondern auch, dass die Kunden vor den Folgen eines Bankverstoßes geschützt sind.

Es gibt verschiedene Key Player:

In UK beispielsweise ist die Financial Conduct Authority (FCA) die oberste Behörde für den Banken- und Finanzsektor. Ihre Hauptaufgabe ist der Schutz der Verbraucher und ihrer Finanzen. Deshalb geht sie gegen Regelverstöße und institutionelle Fehler vor.

Die FCA ist befugt, Finanzprodukte zu verbieten, Einzelheiten über irreführende Finanzwerbung zu veröffentlichen, Verstöße gegen die Sorgfaltspflicht aufzudecken und Informationen über etwaige Disziplinarmaßnahmen zu veröffentlichen. Dazu gehört neben Geldstrafen auch der Entzug von Zulassungen.

Weitere Institutionen sind die Regulierungsbehörde für Zahlungsdienste (Payment Services Regulator – PSR), die für die Aufsicht über alle Massenzahlungssysteme zuständig ist, und der Financial Ombudsman Service (FOS), der von Rechts wegen dafür verantwortlich ist, Beschwerden und Entschädigungsansprüche zu bearbeiten.

Darüber hinaus hat der FOS die Befugnis, Streitigkeiten zu schlichten und Vergleiche zu schließen. Obwohl er eine unabhängige Institution ist, besteht zwischen ihm und der FCA eine Absichtserklärung, so dass der FOS bedeutenden Einfluss auf die Privatkundenbanken nimmt.

Das britische Finanzministerium (HM Treasury) ist insgesamt für die institutionelle Struktur des Bankwesens und die Regulierung zuständig und berichtet dem Parlament über schwerwiegende Probleme im Finanzsystem und die erforderlichen Maßnahmen zu deren Lösung. Wichtig zu wissen ist auch, dass das Finanzministerium die Widerstandsfähigkeit des Bankensektors überwacht und die Verantwortung für die Bewältigung von Betriebsunterbrechungen übernimmt – was während der Pandemie sehr deutlich wurde.



Gängige Fehler

Immer strengere Vorschriften führen zu einem deutlichen Rückgang von Datenmissbrauchsfällen. Kunden und ihre Bankdaten sind gut geschützt. Die meisten Geldstrafen entstehen durch Versäumnisse bei der Geldwäschebekämpfung.

In einem Bericht von Which? aus Januar 2022 war jedoch von Governance-Mängeln bei Apps und Online-Diensten die Rede. Dabei ging es in erster Linie um Versäumnisse bei der Implementierung ausreichend sicherer Passwörter und Verschlüsselungen, aber auch um unsichere Websites, was auf eine schlecht eingerichtete Infrastruktur schließen lässt. Dies könnte ein direktes Ergebnis beschleunigter oder überstürzter digitaler Transformationsprozesse durch zögerliche Betreiber sein.

Besorgniserregend ist, dass den fünfzehn untersuchten Großbanken zu geringer Login-Schutz, eine wenig intuitive App-Navigation und niedrige Benutzerfreundlichkeit bei der plattformübergreifenden Kontoverwaltung bescheinigt wurde. Im Verlauf der Untersuchung stellte sich außerdem heraus, dass eine der konkurrierenden Banken nicht jedes Mal zum Login aufforderte, wenn ein Nutzer auf sein Konto zugriff. Hier kann man nur von einem Versagen der Sorgfaltspflicht einer Bank sprechen.

Natürlich gab es auch Banken, die sehr gut abschnitten, aber das Ausmaß der genannten Probleme gab Anlass zur Sorge. Noch hat die Analyse keine Geldstrafen nach sich gezogen – es ist nicht klar, wie die FCA die Ergebnisse nutzen und zu gegebener Zeit handeln wird.

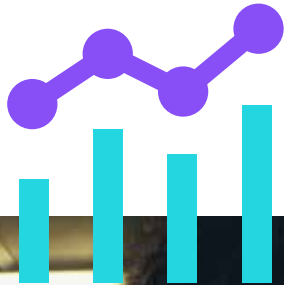


Abschließendes Fazit

Es ist wichtig festzustellen, dass gute Nachrichten selten in die Nachrichten kommen. Eine schlechte Infrastruktur, die Brüche und Schwachstellen verursacht, sollte nicht das Verhalten einer Bank bestimmen. Denn schließlich muss die berechtigte Sorge über die Auswirkungen betrieblicher Schwierigkeiten durch die Beseitigung der Ursachen gelöst werden – und die liegen bei den technischen und Governance-Teams.

Interne Diskussionen müssen sich vielmehr darauf konzentrieren, wie Banken agiler mit Kundendaten umgehen und gleichzeitig die geltenden strengen Vorschriften einhalten können. Militärische Sicherheit bedeutet hier, komplexe Datenanalysen entstehen zu lassen, die es Banken ermöglichen, jeden Kunden besser als je zuvor zu verstehen.

Basierend auf diesen Erkenntnissen wird die Bank zu einem lebenslangen Partner – und profitiert von wachsenden Investitionen. Darüber hinaus kann sich die Bank als zentrale Plattform innerhalb der Marketingstrategie jeder beliebigen Marke positionieren – schließlich haben die Verbraucher den Wunsch geäußert, dass ihre Daten zu ihrem eigenen Vorteil genutzt werden.



Die Tools sind vorhanden, um Kunden besser als je zuvor zu verstehen. Banken müssen in ihrem Ansatz mutiger sein, um im Jahr 2022 und darüber hinaus wettbewerbsfähig zu bleiben. Die Angst vor Übertretungen darf sie nicht von den unzähligen Möglichkeiten abhalten, die direkt vor ihrer Nase liegen.





Wir verbinden Daten, damit Sie sich mit Ihren Kunden verbinden können
Tag Management | API Hub | Customer Data Platform und Machine Learning | Data Management

Tealium verknüpft Kundendaten – über Web-, Mobil-, Offline- und IoT-Geräte, damit Marken sich mit ihren Kunden verbinden können. Das schlüsselfertige Integrations-Ökosystem von Tealium unterstützt über 1.300 client- und serverseitige Anbieter und Technologien und ermöglicht es Marken, eine einheitliche Echtzeit- Kundendateninfrastruktur zu schaffen. Der Tealium Customer Data Hub umfasst ein Tag-Management, einen API-Hub, eine Customer Data Platform mit Machine Learning und Datenmanagementlösungen, die Kundendaten wertvoller, praktikabler und sicherer machen. Mehr als 850 Unternehmen weltweit vertrauen Tealium, ihre Kundendaten- Strategien voranzutreiben.

Weitere Informationen unter

tealium.de