Fabian Leonhardt / Arnd Wiedemann

Digitalisierung und Personalisierung im Spannungsfeld von Kunden- und Bankinteressen

Kunden erwarten auch von ihrem Finanzdienstleister und damit von Sparkassen, Genossenschaftsbanken und Großbanken immer stärker die Leistungen und Annehmlichkeiten, die sie im Internet erleben. Dies machen sich die digitalen Wettbewerber der klassischen Universalbanken zunutze und bieten auf Basis von Informations- und Kommunikationstechnologien Bankleistungen digital beziehungsweise auf digitaler Basis an.[1] Diese Fähigkeit der digitalen Wettbewerber, den Wunsch der Kunden nach Bequemlichkeit in besonderem Maße zu erfüllen und gleichzeitig die Leistungen kostengünstig anzubieten, stellt zunächst einmal eine Bedrohung für Universalbanken dar. Doch Sparkassen, Genossenschaftsbanken und Großbanken verfügen nach wie vor über Wettbewerbsvorteile gegenüber der digitalen Konkurrenz. Werden diese Wettbewerbsvorteile geschickt mit den neuen Technologien kombiniert, eröffnen sich neue Erfolgspotenziale für die Zukunft. Abbildung 1 verdeutlicht diese als Schnittmenge, die sich ergibt, wenn die Wettbewerbsvorteile mit den Potenzialen der modernen Informations- und Kommunikationstechnologien kombiniert werden.

Vertrauensvorschuss der Banken beim Datenschutz

Geht der Verbraucher noch relativ sorglos mit der Frage um, was Google, Amazon oder Facebook mit den Daten machen, die sie sammeln, wie sie diese auswerten, nutzen und gegebenenfalls auch verkaufen, und gibt er bereitwillig bewusst oder unbewusst Informationen über sich preis, zum Beispiel welches Filmgenre, welche Sportarten oder Modelabels er mag oder wann und wo die jeweiligen Dienste genutzt werden, so reagieren Kunden wesentlich sensibler, wenn es um ihre finanzbezogenen Daten geht.[2] In der Internetökonomie, und damit zum Beispiel für Google oder Facebook, stellen Daten die zentrale Währung dar und sind integraler Bestandteil ihrer Geschäftsmodelle. Nur bei den Kriterien Datensicherheit und Datenschutz werden Banken und Sparkassen als zuverlässiger und vertrauenswürdiger eingeschätzt als ihre digitalen Wettbewerber.[3]

Ein weiterer Vorteil von Banken und Sparkassen gegenüber ihren digitalen Wettbewerbern ist, dass sie über eine große Kundenbasis verfügen und für die deutliche Mehrheit der Privatkunden in Deutschland die Hausbank darstellen. Direktbanken gelingt es trotz ihrer Markterfolge nicht nachhaltig und durchdringend eine Hausbankbeziehung zu ihren Kunden aufzubauen.[4] Als Hausbankverbindung verfügen Banken und Sparkassen aber über einen immensen Datenschatz.

Digitale Wettbewerber stehen zudem vor der Herausforderung, wie sie den Bedarf der Kunden nach Individualisierung im Sinne eines geeigneten Zuschnitts erfüllen.[5] Banken und Sparkassen verfügen über die dazu erforderlichen Daten. Lediglich die Technologien zur effektiven und effizienten Umsetzung fehlen (noch). Darüber hinaus suchen Kunden gerade bei komplizierteren Produkten, wie zum Beispiel der Altersvorsorge, der Immobilienfinanzierung oder der Vermögensanlage, weiterhin den direkten menschlichen Kontakt in der Filiale oder über den mobilen Vertrieb.[6]

Nachholbedarf beim Cross-Selling

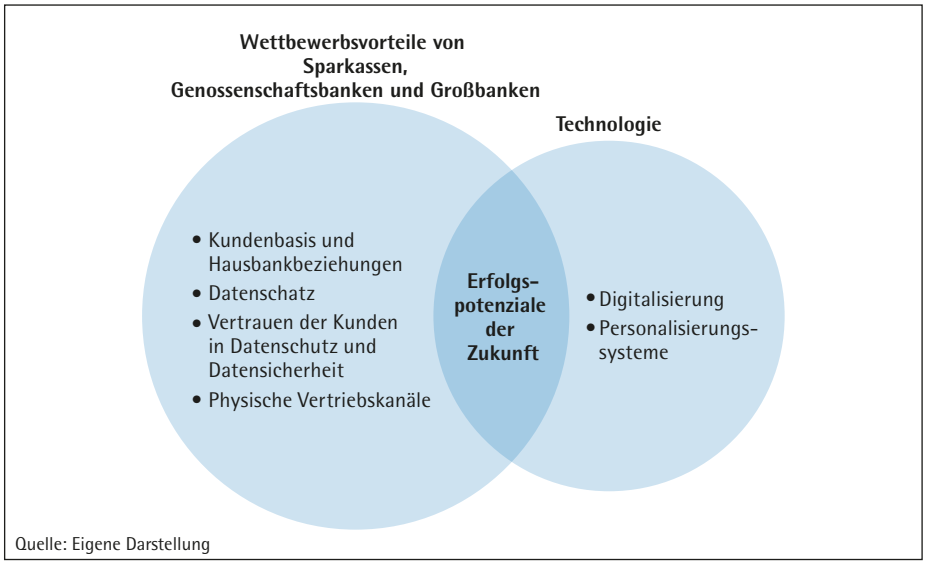
Besonders bei der Ausschöpfung der Cross-Selling-Potenziale des Kundenbestands haben deutsche Banken und Sparkassen aber Nach- und Aufholpotenzial.[7] Dieses Potenzial kann durch die Sammlung und

Prof. Dr. Arnd Wiedemann, Inhaber des Lehrstuhls für Finanz- und Bankmanagement, Universität Siegen, Fabian Leonhardt, wissenschaftlicher Mitarbeiter des Lehrstuhls

Ihrem Vertrauensvorschuss in puncto Datenschutz und Datensicherheit, aber auch dem Umfang ihrer Daten nach schreiben die Autoren der Kreditwirtschaft durchaus gute Chancen im Wettbewerb mit branchenfremden Anbietern auch in Zeiten der Digitalisierung erfolgreich standzuhalten. Sie mahnen aber an, mit ihrem Datenschatz sehr verantwortungsvoll umzugehen und nicht nur den datenschutzrechtlichen Rahmen, sondern auch die moralische Erwartung der Kunden penibel einzuhalten. Im Zweifel empfehlen sie, bei der Erstellung und Nutzung von Kundenprofilen die Einwilligung einzuholen. Als Möglichkeit, die Interessen von Kreditinstituten und Kunden in Einklang zu bringen, empfehlen sie das Permission Marketing als mögliche Lösung. Insbesondere bei technikaffinen und vielleicht abwanderungsgefährdeten Kunden versprechen sie sich davon jedenfalls einen Zusatznutzen für beide Seiten. (Red.)

-nutzung von Daten, digitale Vertriebswege und Touchpoints und deren Personalisierung gehoben werden. Es gilt, auf Basis der Informations- und Kommunikationstechnologie die Effektivität der vertrieblichen Maßnahmen zu erhöhen und die möglichen Effizienzpotenziale zu nutzen.[8] Beispielsweise besteht die Möglichkeit, die verfügbaren internen und externen Daten der Kundenbeziehungen zu nutzen und sie mit den Potenzialen erfolgreicher Personalisierungssysteme und -techniken der Internetökonomie, wie zum Beispiel Empfehlungssystemen, zu kombinieren.[9] Insofern stellt die Digitalisierung und die damit verbundene Personalisierung von Leistungen und Touchpoints auf Basis des vorhandenen Datenschatzes, kombiniert mit den zuvor genannten Wettbewerbsvorteilen, für Banken und Sparkassen eine große Chance dar.

Abbildung 1: Erfolgspotenziale der Zukunft von Sparkassen, Genossenschaftsbanken und Großbanken



Quelle: Eigene Darstellung

Der Schlüssel zur Wahrnehmung dieser Chance ist der Zugang zum Kunden und zu dessen Daten. Diese sind die Grundlage, um Kunden passgenau, bedarfsgerecht und bequem mit Leistungen zu bedienen und somit die Voraussetzung, um dessen Ertragspotenziale auszuschöpfen. Doch neben der Attraktivität der Datenverwendung aus Sicht der Bank oder Sparkasse ist das Interesse der Kunden im Sinne moralischer Erwartungen zum Umgang mit den (sensiblen finanzbezogenen) Daten und datenschutzrechtlichen Vorgaben zu berücksichtigen. Sollte das bestehende Vertrauen der Kunden in den Datenschutz und die Datensicherheit gegenüber Banken und Sparkassen verloren gehen, kann auch der Zugang zum Kunden und dessen Daten gänzlich verloren gehen. Damit kann ein zentraler Wettbewerbsvorteil zunichtegemacht werden. Dem geltenden Datenschutzrecht sowie den Erwartungen der Kunden zum Umgang mit den Daten ist daher besondere Aufmerksamkeit zu schenken.

Das Vertrauen der Kunden in Banken und Sparkassen hat besonders in den vergangenen zehn Jahren durch die Finanzkrise und verschiedene Fälle rechtlicher und moralischer Verstöße gelitten. Weitere derartige Verstöße, insbesondere im Umgang mit Daten, können den noch bestehenden Vertrauensvorschuss gegenüber den neuen, digitalen Wettbewerbern der Finanzbranche aufs Spiel setzen. Sparkassen, Genossenschaftsbanken und Großbanken müssen daher proaktiv ihr Interesse an der Sammlung und Nutzung von internen und externen Kundendaten mit den Interessen und Erwartungen ihrer Kunden sowie den datenschutzrechtlichen Vorgaben in Einklang bringen.

Kundendaten der Banken

Der zentrale Rohstoff, um die Wettbewerbsvorteile von Banken und Sparkassen mit den Chancen der Technologie und der Digitalisierung zu Erfolgspotenzialen zu kombinieren, sind die Daten der Kunden. Im Gegensatz zu anderen Branchen und auch zum digitalen Wettbewerb verfügen Sparkassen, Genossenschaftsbanken und Großbanken über eine umfassende Datenbasis ihrer Kunden.

Daten, die Banken und Sparkassen über Kunden intern und extern erheben und verarbeiten können, lassen sich allgemein in Deskriptionsdaten, Identifikationsdaten und Transaktionsdaten aufspalten.[10] Dabei stellen Identifikationsdaten klassischerweise Kundenstammdaten dar. Deskriptionsdaten beinhalten Daten zu demografischen, psychografischen und/oder soziografischen Kundeneigenschaften. Transaktionsdaten beziehen sich auf die Geschäftsbeziehung zwischen Kunde und Bank beziehungsweise Sparkasse. Insbesondere durch die Produktnutzung fallen zahlreiche Transaktionsdaten an.

Auch die Nutzung der digitalen Zugangswege wie das Internet Banking oder digitale Leistungen wie das Online Banking und das Mobile Banking liefern Transaktionsdaten. Diese Daten können im Rahmen der internen Kundenbeziehung oder durch externe Quellen (zum Beispiel Internet oder soziale Medien) generiert werden, indem sie manuell durch Mitarbeiter und/oder automatisiert und digital auf Basis von Informations- und Kommunikationstechnologien erhoben und gesammelt werden.

Mit den internen und externen Daten lassen sich Kundenprofile erstellen, die die Basis für eine proaktive Bedarfs- und Präferenzidentifikation bilden.[11] Diese Kunden- oder auch Nutzerprofile stellen wiederum die Basis der (digitalen) Personalisierungssysteme dar, um Leistungen, Produkte aber auch Touchpoints proaktiv und automatisiert auf Kunden und deren Bedarfe und Präferenzen zuschneiden zu können.

Moralische Erwartung der Kunden

Maßgeblich für die Zulässigkeit der Erhebung und Nutzung dieser Daten und der Erstellung von Kunden- beziehungsweise Nutzerprofilen sind die datenschutzrechtlichen Vorgaben sowie die moralischen Erwartungen der Gesellschaft und Kundschaft gegenüber ihrem Finanzdienstleister. Beide Aspekte bilden die Leitplanken im Umgang mit den Kundendaten, die es vor der Nutzung der Kundendaten im Interesse der Bank oder Sparkasse zu berücksichtigen gilt.

Bevor die relevanten datenschutzrechtlichen Normen dargelegt werden, sei zunächst auf die moralischen Erwartungen der Kunden eingegangen. Maßgebend ist zum einen die Sensibilität für das Eindringen in die Privatsphäre des Kunden und zum anderen die wahrgenommene Aufdringlichkeit werblicher und vertrieblicher Ansprachen. Besonders in der europäischen und deutschen Gesellschaft ist die Befürchtung, zum gläsernen Menschen beziehungsweise zum gläsernen Kunden zu werden, verbreitet.

Wie erwähnt, verfügen Sparkassen, Genossenschaftsbanken und Großbanken in der Wahrnehmung ihrer Kunden über einen Vorsprung an Seriosität und Diskretion gegenüber den digitalen Wettbewerbern. Kunden vertrauen darauf, dass ihre Bank oder Sparkasse mit ihren Daten vertraulich und verantwortungsvoll umgeht.[12] Wird dieses Vertrauen verletzt, drohen neben möglichen rechtlichen Sanktionen in jedem Falle Reputationsschäden und damit der bereits erwähnte mögliche Verlust des wettbewerblichen Vorteils gegenüber den digitalen Wettbewerbern.

Eindringen in die Privatsphäre der Kunden

Das wahrgenommene Eindringen in die Privatsphäre kann anhand von vier Merkmalen betrachtet werden (vergleiche Abbildung 2). Die konkrete Ausprägung dieser Merkmale zeigt an, wie stark die Kundenprofile und die Personalisierung in die Privatsphäre eines Kunden eindringen.[13]

Abbildung 2 zeigt, dass der Grad des Eindringens abhängig ist von der eingesetzten Erhebungsmethode, der Verwendungsdauer, der Beteiligung des Kunden sowie der genutzten Analysemethode.[14] Werden Kundenprofile implizit aus dem Verhalten der Kunden gegenüber ihrer Bank oder Sparkasse, wie zum Beispiel aus der Produktnutzung, abgeleitet, sind sich Kunden der erhobenen Daten im Detail weniger bewusst, was zu einem stärkeren Eindringen in die Privatsphäre führt. Da es bei Kundenprofilen üblich ist, die Daten der Kunden dauerhaft zu verwenden und laufend anzupassen, wird ebenfalls stärker in die Privatsphäre der Kunden eingedrungen, als wenn dies nur einmalig oder vorübergehend geschieht.

Ferner gilt, je weniger aktiv Kunden an der Datenverwendung beteiligt sind und je mehr systembasiert und automatisiert Daten verwendet werden, desto mehr dringt die Datenverwendung in die Privatsphäre ein. Auch der Einsatz von Analysemethoden, die Prognosen zum Verhalten des Kunden zur Nutzung von Produkten oder Touchpoints erstellen, führt zu einem stärkeren Eindringen in die Privatsphäre.

Die Ausprägungen der Merkmale in Abbildung 2 geben zunächst wieder, wie stark Kundenprofile und eine darauf basierende Personalisierung in die Privatsphäre eindringen. Sie zeigen aber gleichzeitig auch Handlungsimplikationen auf. Wird der Grad der angestrebten bankseitigen Personalisierung abgeschwächt, reduziert sich zwar das Ausmaß des Eindringens in die Privatsphäre, gleichzeitig leidet damit aber auch die Qualität und Effektivität der Personalisierung. Alternativ kann angestrebt werden, möglichst offen und transparent mit den verwendeten Daten der Kunden umzugehen und die Kunden gegebenenfalls sogar in den Prozess miteinzubeziehen.[15] Allerdings sind der Transparenz insofern auch Grenzen gesetzt, als damit Prozesse und Techniken der Datenverwendung und Personalisierung für die Wettbewerber offengelegt würden.

Datenschutzrechtliche Situation beachten

Zur datenschutzrechtlichen Betrachtung ist zwischen dem Eindringen in die Privatsphäre durch die Erstellung und Nutzung von Kundenprofilen (zur Personalisierung) sowie der Aufdringlichkeit durch eine proaktive Kundenansprache zu differenzieren.[16]

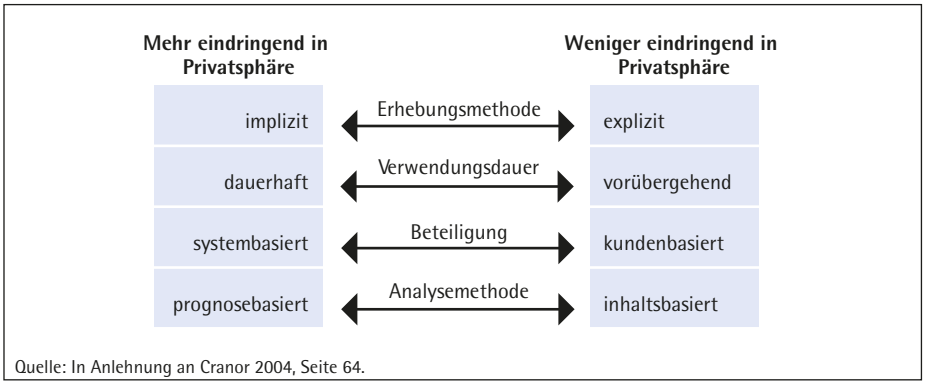
Allgemein wird Datenschutz in Deutschland durch das Bundesdatenschutzgesetz (BDSG) geregelt, sofern keine bereichsspezifischen Gesetze gelten. Das Eindringen in die Privatsphäre wird im Wesentlichen durch das BDSG sowie das Telemediengesetz (TMG) geregelt. Das TMG behandelt bereichsspezifisch datenschutzrechtliche Aspekte von Telemedienangeboten, wie zum Beispiel Homepages, Webshops, Suchmaschinen, Bewertungsportalen oder auch dem Internet Banking, Online Banking und Mobile Banking.[17] Die zulässige Aufdringlichkeit durch werbliche Ansprachen wird durch das Gesetz gegen den unlauteren Wettbewerb (UWG) geregelt.

Prinzipiell gilt im deutschen Datenschutzrecht ein Verbot mit Erlaubnisvorbehalt, wonach die Erhebung, Verarbeitung und Nutzung personenbezogener Daten verboten ist, es sei denn, ein gesetzlicher Erlaubnistatbestand sieht eine zulässige Verwendung vor oder die Kunden haben dazu ihre ausdrückliche Einwilligung gegeben.

Personenbezogene Daten stellen nach § 3 Abs. 1 BDSG Einzelangaben über persönliche und sachliche Verhältnisse einer natürlichen Person dar. Dazu gehören neben dem Namen beispielsweise die Adresse, die Berufsbezeichnung, das Einkommen, Online-Nutzungsdaten sowie Geo- oder Bewegungsdaten. Bei den Daten des Bankgeschäfts handelt es sich typischerweise um personenbezogene Daten.

Gleiches gilt für externe Daten von Kunden, die nicht aus der unmittelbaren Geschäftsbeziehung mit den Kunden resultieren, sondern aus externen Quellen, wie zum Beispiel sozialen Medien, bezogen werden. Von den personenbezogenen Daten sind anonyme und pseudonyme Daten abzugrenzen, die aus dem Geltungsbereich

Abbildung 2: Merkmale des Eindringens in die Privatsphäre

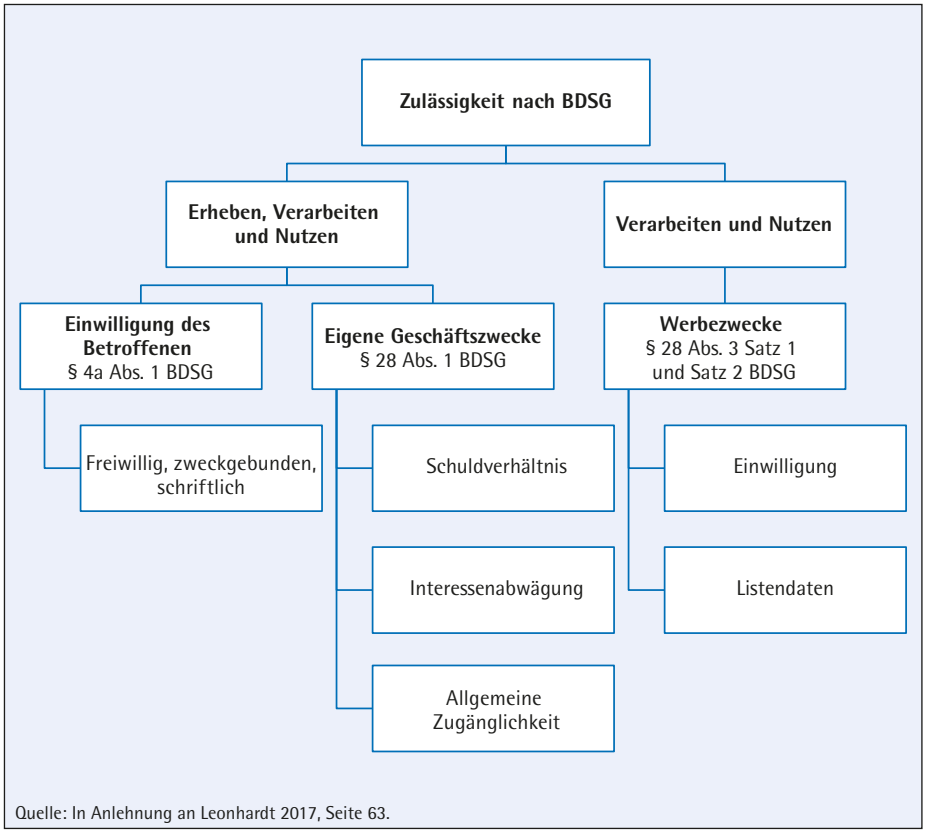


Quelle: In Anlehnung an Cranor 2004, Seite 64.

des BDSG herausführen beziehungsweise dessen Vorgaben abmildern können.

Zur groben Differenzierung der Gültigkeitsbereiche zwischen BDSG und TMG regelt das BDSG die Zulässigkeit der Verwendung personenbezogener Daten im Offlinebereich, während das TMG die Zulässigkeit der Verwendung personenbezogener Daten im Onlinebereich regelt.[18] Eine Ausnahme von dieser Abgrenzung stellen die sogenannten Inhaltsdaten des Onlinebereichs dar, die durch das BDSG erfasst werden. Dazu gehören beispielsweise online erstellte Inhalte, die auch als User Generated Content (UGC) bezeichnet werden.[19] Inhaltsdaten des Online Bankings oder des Mobile Bankings, wie zum Beispiel der aktuelle Kontostand oder vergangene Transaktionen, fallen damit in den Gültigkeitsbereich des BDSG. Die sogenannten Bestands- und Nutzungsdaten sind hingegen dem Gültigkeitsbereich des TMG zuzuordnen. Bezogen auf das Beispiel des Online Bankings beziehungsweise des Mobile Bankings können dies die PIN, die IP-Adresse, die verwendete TAN, die Dauer und der Verlauf des Klickstreams der Onlinenutzung sowie die Standortdaten der Nutzung sein.

Abbildung 3: Zulässigkeit der Verwendung personenbezogener Kundendaten nach dem Bundesdatenschutzgesetz (BDSG)



Quelle: In Anlehnung an Leonhardt 2017, Seite 63.

Einwilligung, eigene Geschäftszwecke sowie Werbezwecke

Abbildung 3 stellt die jeweiligen Rechtsnormen zur Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach dem BDSG dar. Danach unterscheidet das BDSG im Wesentlichen drei Möglichkeiten der Zulässigkeit: Einwilligung, eigene Geschäftszwecke sowie Werbezwecke. Dabei ist die Trennung der Datenverwendungsstufen in Form der Erhebung, Verarbeitung und Nutzung zu berücksichtigen, die auch im Rahmen der Zulässigkeit aufeinander aufbauen.[20] § 4a Abs. 1 BDSG regelt die Einwilligung des Kunden in die Datenerhebung, -verarbeitung und -nutzung als Opt-in. Die Einwilligung erfolgt freiwillig sowie schriftlich und muss den Zweck der Verwendung der personenbezogenen Daten beinhalten. Eine Zweckänderung ist insofern nur mit Einwilligung des Kunden möglich.

§ 28 Abs. 1 BDSG regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Kundendaten für eigene Geschäftszwecke und nennt dabei wiederum drei Erlaubnistatbestände, die eine Datenverwendung auch ohne Einwilligung des Kunden möglich machen. Dazu gehören das Schuldverhältnis, die Interessenabwägung und die allgemeine Zugänglichkeit. Ferner erlaubt § 28 Abs. 3 Satz 1 BDSG die Verarbeitung und Nutzung für Werbezwecke, sofern die betroffene Person eingewilligt hat. Nach § 28 Abs. 3 Satz 2 BDSG dürfen so genannte Listendaten auch ohne Einwilligung des Betroffenen zu Werbezwecken verwendet werden, sofern kein Widerspruch erfolgt.[21]

Verbotsprinzip mit Erlaubnisvorbehalt

Für Bestands- und Nutzungsdaten des Onlinebereichs gilt das TMG. Auch für das TMG hat das Verbotsprinzip mit Erlaubnisvorbehalt Gültigkeit. Nach § 12 TMG dürfen personenbezogene Daten verwendet werden, wenn eine Einwilligung des Betroffenen vorliegt oder Erlaubnistatbestände es zulassen. Personenbezogene Bestandsdaten dürfen nach § 14 Abs. 1 TMG zweckgebunden zur Begründung, Abwicklung oder Änderung eines vertraglichen Verhältnisses zur Nutzung von Telemedien herangezogen werden. Nutzungsdaten dürfen nach § 15 Abs. 1 Satz 1 TMG nur verwendet werden, wenn sie erforderlich sind, um die Nutzung der Telemedien durch den Nutzer zu ermöglichen und/oder die Nutzung abzurechnen. Sofern Nutzungsdaten zu sogenannten Nutzungsprofilen aggregiert und zum Zwecke der Werbung, Marktforschung oder der bedarfsgerechten Gestaltung des Telemediums genutzt werden, sind die Nutzungsprofile nach § 15 Abs. 3 TMG zu pseudonymisieren, sofern der Nutzer der Erzeugung der Nutzungsprofile nicht widerspricht (Opt-out).

Sofern die personenbezogenen Daten zur Personalisierung zulässig erhoben, verarbeitet und genutzt werden dürfen, können diese zur Personalisierung und proaktiven Kundenansprache eingesetzt werden. Die Zulässigkeit einer proaktiven Kundenansprache regelt in Abhängigkeit des Ansprachemediums das UWG. Nach § 7 Abs. 2 Nr. 2 und Nr. 3 UWG muss bei Ansprachen per Telefon, per E-Mail, per SMS sowie per Instant Message eine Einwilligung (Opt-in) des Kunden vorliegen.[22] Lediglich der Briefversand an Bestandskunden ist nach

§ 28 Abs. 3 Satz 2 Nr. 1 Alt. 1 BDSG legitimiert, sofern kein Widerspruch des Kunden erfolgt.[23)]

Eine Bank oder Sparkasse muss also am konkreten Einzelfall detailliert abwägen, welcher Grad an Personalisierung bankseitig gewünscht ist, welche personenbezogenen Daten dazu erforderlich und verfügbar sind und wie diese Daten zulässig verwendet werden dürfen. Sofern personenbezogene Daten erforderlich sind und damit Kundenprofile erstellt werden, die verschiedene personenbezogene Daten aus unterschiedlichen Quellen abbilden, ist zu prüfen, welche der skizzierten datenschutzrechtlichen Vorgaben betroffen sind, welche gesetzlichen Zulässigkeitstatbestände gegebenenfalls greifen und wie die Einwilligungserklärung rechtskonform auszugestalten ist. Dabei ist auch die Art der Kommunikation der Personalisierung zu berücksichtigen, die in Abhängigkeit des Mediums und der Proaktivität die Einwilligung des Kunden erforderlich machen kann.

Einwilligung bei Erstellung und Nutzung von Kundenprofilen

Zwar ermöglicht ein Abstellen auf die Zulässigkeitstatbestände nach § 28 Abs. 1 und Abs. 3 BDSG prinzipiell die Verwendung personenbezogener Daten, ohne dass eine Anonymisierung der Daten oder eine Einwilligung des Kunden erforderlich ist. Allerdings sind diesen Zulässigkeitstatbeständen enge Grenzen gesetzt. Daten des Onlinebereichs, die in den Gültigkeitsbereich des TMG fallen, wie zum Beispiel Nutzungsdaten, sind ohnehin nur pseudonymisiert verwendbar. Eine Datenanonymisierung und -pseudonymisierung geht mit einem Informationsverlust einher, der es erschwert oder gar unmöglich macht, auf Basis von Kundenprofilen spezifische Bedarfe abzuleiten, Präferenzen zu identifizieren und Kunden passgenau und personalisiert anzusprechen.[24)]

Die engen Grenzen des Datenschutzrechts führen also dazu, dass nicht alle im Rahmen der Kundenbeziehung verfügbaren sowie zusätzlichen externen Daten ohne die Einwilligung des Kunden verwendet werden dürfen. Das Abstellen auf die Zulässigkeitstatbestände bedeutet zudem nicht gleichzeitig und automatisch, dass eine mögliche und rechtlich zulässige Datenverwendung auch zwangsläufig moralisch legitim ist. Hier sind insbesondere die datenschutzrechtlichen Grauzonen angesprochen.

Einholen einer Einwilligung

Nach Plath ergibt sich aus den Erlaubnistatbeständen des § 28 BDSG keine Zulässigkeit zur Erstellung und Nutzung von Kundenprofilen, womit eine Einwilligung des Kunden erforderlich ist.[25)] Lang empfiehlt daher ausdrücklich auf die explizite Einwilligung des Kunden abzustellen.[26)] Auch nach dem UWG ist für die im Rahmen der Digitalisierung relevanten Ansprachemedien eine Einwilligung des Kunden erforderlich.

Das Einholen einer Einwilligung stellt nicht nur die erforderliche datenschutzrechtliche Zulässigkeit der Verwendung von Kundenprofilen her, sondern schafft gleichzeitig auch die erforderliche moralische Legitimation. So kann proaktiv Akzeptanz aufseiten des Kunden geschaffen werden und dieser über den Nutzen und Mehrwert der Datenverwendung und auch den Aufwand und die Anstrengungen, die eine Bank oder Sparkasse unternimmt, um passgenaue Leistungen anzubieten, informiert werden.

Permission Marketing

Allerdings stellt eine Einwilligung des Kunden im Umkehrschluss auch keinen Freibrief für eine systematische und umfassende Datenverwendung dar. Denn auch hier sind die gesetzlichen Vorgaben einer gültigen Einwilligungserklärung zu berücksichtigen und deren Formulierung ist unter Abwägung von Kunden- und Bankinteressen rechtsgültig auszugestalten. Ferner muss der Sinn und Zweck der Einwilligung gegenüber dem Kunden erläutert werden, damit dieser bereit ist, die Erlaubnis zu erteilen. Dazu ist der Nutzen der Einwilligung und damit auch der Personalisierung aufzuzeigen.[27)] In diesem Zusammenhang stellt das Permission Marketing ein Konzept dar, das eine Lösung bietet, um Kunden- und Bankinteressen in Einklang zu bringen.[28)] Das Permission Marketing zielt auf die ausdrückliche Erlaubnis des Kunden zur Datenverwendung und Kundenansprache ab.[29)]

Die drei konstitutiven Merkmale des Permission Marketings stellen die Personalisierung, die Antizipation sowie die Relevanz dar.[30)] Personalisierung bedeutet, dass die Maßnahmen und Leistungen auf den Kunden zugeschnitten beziehungsweise personalisiert sind. Die Antizipation beinhaltet, dass Kunden diese Personalisierung erwarten. Und schließlich beinhaltet die Relevanz, dass die Personalisierung für den Kunden von Interesse beziehungsweise Bedeutung ist. Diese drei Merkmale decken sich mit den Zielen der Personalisierung und dem Einsatz von Personalisierungssystemen im Rahmen der Digitalisierung.[31)] Das Permission Marketing bewirkt durch die explizite Erlaubnis eine Antizipation der Personalisierung, sodass Kunden die Personalisierung nicht mehr als ein- und aufdringlich empfinden, sondern diese im Gegenteil sogar erwarten. Darüber hinaus können durch die Einwilligung auch gleichzeitig die datenschutzrechtlichen Anforderungen an eine zulässige Datenverwendung erfüllt werden.

Ferner ist es im Rahmen des Permission Marketings möglich, Kunden an ihrem Kundenprofil mitarbeiten und präferierte Touchpoints bestimmen zu lassen, wodurch die Personalisierung und deren Relevanz vom Kunden aktiv beeinflusst werden kann. Demnach ist es auch möglich, Kunden entscheiden zu lassen, was in ihrem Profil gespeichert und verarbeitet wird, wodurch weitere Akzeptanz geschaffen und eine noch effektivere Personalisierung möglich wird. Natürlich wird es nicht allen Kunden leichtfallen, an ihrem eigenen Kundenprofil mitzuarbeiten, und natürlich werden nicht alle Kunden dies wünschen und auch wollen.[32)] Dennoch kann dies gerade für junge und technikaffine Kunden einen interessanten Zusatznutzen darstellen, weil es ihnen Spaß macht. Auch ist hierbei zu berücksichtigen, dass die Transparenz gegenüber Kunden dort an ihre Grenzen stößt, an denen bankinterne Geschäftsgeheimnisse offengelegt werden.

Strategisches Umdenken erforderlich

Damit Sparkassen, Genossenschaftsbanken und Großbanken, deren Geschäftsmodell der Idee der Universalbank folgt, ihre Marktposition gegenüber den digitalen Wettbewerbern, die sich auf spezielle Segmente, Produkte und/oder Vertriebswege fokussieren, aufrechterhalten können, gilt es, die bestehenden Wettbewerbsvorteile in Gestalt der Hausbankbeziehung, der Kundennähe, des Datenschatzes, des Vertrauens der Kunden in Datenschutz und Datensicherheit und der physischen Ver-

triebskanäle zu nutzen. Im Rahmen der fortschreitenden Digitalisierung und der damit möglichen Personalisierung von Leistungen und Touchpoints können bisher nicht ausgeschöpfte Vertriebs- und Cross-Selling-Potenziale im Kundenbestand gehoben werden. Dabei gilt vereinfacht, je besser und umfassender das Kundenprofil ist, desto effektiver wird die Personalisierung und damit der Zuschnitt der Leistungen auf den Bedarf und die Präferenzen der Kunden.

Die Zulässigkeit eines umfassenden und systematischen Sammelns von Daten zur Erzeugung dauerhafter Kundenprofile lässt sich aus den Erlaubnistatbeständen des BDSG und TMG nicht ableiten, sodass eine Einwilligung des Kunden erforderlich ist. Dies ist im Hinblick auf die moralischen Erwartungen der Kunden aber ohnehin empfehlenswert.

In diesem Sinne empfiehlt sich ein strategisches Umdenken. Die Einwilligung des Kunden sollte nicht als notwendiges Übel empfunden werden, sondern aktiv in den Vertriebsprozess eingebunden werden. Sie schafft im Rahmen des Permission Marketings Akzeptanz und bietet den geeigneten Anlass, den Kunden den Nutzen von Kundenprofilen und der Personalisierung und damit letztlich den Mehrwert für sie aufzuzeigen. Dies bietet einer Bank oder Sparkasse darüber hinaus die Chance, gerade jungen und technikaffinen und vielleicht abwanderungsgefährdeten Kunden einen Zusatznutzen zu bieten und das Institut neu zu positionieren.

Literatur

Arndt, D. (2011): Datenschutzaspekte in CRM Projekten, in: Hippner, H.; Hubrich B.; Wilde, K. D. (Hrsg.): Grundlagen des CRM: Strategie, Geschäftsprozesse und IT-Unterstützung, 3. Auflage, Wiesbaden, S. 182 bis 209.

Bragge, J.; Sunikka, A.; Kallio, H. (2012): An Exploratory Study on Customer Responses to Personalized Banner Messages in the Online Banking Context, in: Journal of Information Technology Theory Application, 13. Jg., Nr. 3, S. 5 bis 20.

Bunzel, M.; Gaess, W. (2013): Rahmenbedingungen und Datenschutzorganisation, in: Berndt, M. (Hrsg.): Datenschutz und IT-Sicherheit: Umsetzungsanleitung und Umsetzungsprüfung für die Praxis von Banken und Sparkassen, 3. Auflage, Heidelberg, S. 3 bis 45.

Cranor, L. F. (2004): I didn't buy it for myself: Privacy and Ecommerce Personalization, in: Karat, M.-C.; Blom, J. O.; Karat, J. (Hrsg.): Designing Personalized User Experience in eCommerce, New York u. a., S. 57 bis 73.

Culmsee, T. (2015): Prinzipien des Datenschutzrechts, in: Dorschel, J. (Hrsg.): Praxishandbuch Big Data: Wirtschaft, Recht, Technik, Wiesbaden, S. 167 bis 174.

Dapp, T. F. (2014): Fintech: Die digitale (R)evolution im Finanzsektor: Algorithmenbasiertes Banking mit human touch, Deutsche Bank Research, 23.09.2014, URL: https://www.dbresearch.de/PROD/DBR_INTERNET_DE-PROD/PROD0000000000342293. pdf, Abrufdatum: 6. Januar 2017.

Dapp, T. F. (2015): Fintech reloaded: Die Bank als digitales Ökosystem: Mit bewährten Walled Garden-Strategien in die Zukunft, Deutsche Bank Research, 28.4.2015, URL: https://www.dbresearch.com/PROD/DBR_INTERNET_DE-PROD/PROD000000000035450 5/Fintech+reloaded+%E2%80%93+Die+Bank+als+digitales+%C3%96kosyste.pdf, Abrufdatum: 6. Januar 2017.

Eckhardt, J. (2015): Big Data im Marketing: Rechtliche Eckpunkte, in: Schwarz, T. (Hrsg.): Big Data im Marketing: Chancen und Möglichkeiten für eine effektive Kundenansprache, Freiburg, S. 270 bis 307.

van Geenen, W.; Dorschel, W.; Dorschel, J. (2015): Big Data in der Kreditwirtschaft, in: Dorschel, J. (Hrsg.): Praxishandbuch Big Data: Wirtschaft, Recht, Technik, Wiesbaden, S. 134 bis 148.

Godin, S. (1999): Permission Marketing: Turning Strangers into Friends, and Friends into Customers, New York.

Gorgoglione, M.; Panniello, U. (2011): Beyond Customer Churn: Generating Personalized Actions to Retain Customers in a Retail Bank by a Recommender System Approach, in: Journal of Intelligent Learning Systems and Applications, 3. Jg., Nr. 2, S. 90 bis 102.

Heckmann, D. (2014): Juris Praxiskommentar Internetrecht: Telemediengesetz, E-Commerce, E-Government, 4. Aufl., Saarbrücken.

Kerner, S. (2002): Analytisches Customer-Relationship-Management in Kreditinstituten: Data Warehouse und Data Mining als Instrumente zur Kundenbindung im Privatkundengeschäft, Dissertation, Wiesbaden.

Köhler, H.; Bornkamm, J. (2016): Gesetz gegen den unlauteren Wettbewerb UWG: mit Preisangabenverordnung, Unterlassungsklagengesetz, Dienstleistungs-Informationspflichten-Verordnung, Kommentar, 34. Auflage, München.

Kumar, V.; Zhang, X. A.; Luo, A. (2014): Modeling Customer Opt-In and Opt-Out in a Permission-Based Marketing Context, in: Journal of Marketing Research, 51. Jg., Nr. 4, S. 403 bis 419.

Lang, M. (2013): Kundendatenschutz, in: Berndt, M. (Hrsg.): Datenschutz und IT-Sicherheit: Umsetzungsanleitung und Umsetzungsprüfung für die Praxis von Banken und Sparkassen, 3. Auflage, Heidelberg, S. 47 bis 93.

Leonhardt, F. (2017): Einsatz von Empfehlungssystemen zur Kundenansprache in Banken: Eine konzeptionelle Untersuchung anhand des Retailgeschäfts traditioneller Universalbanken, Band 18 der Schriftenreihe ccfb – competence center finanz- und bankmanagement, Dissertation, Frankfurt am Main.

Leußer, W.; Hippner, H.; Wilde, K. D. (2011): Kundeninformationen als Basis des CRM, in: Hippner, H.; Hubrich B.; Wilde, K. D. (Hrsg.): Grundlagen des CRM: Strategie, Geschäftsprozesse und IT-Unterstützung, 3. Auflage, Wiesbaden, S. 731 bis 755.

Lieberknecht, J. (2016): Digitalisierung und Regulierung: Katalysatoren eines sich wandelnden Bankgeschäfts, in: Hellenkamp, D.; Fürderer, K. (Hrsg.): Handbuch Bankvertrieb: Theorie und Praxis im Zukunftsdialog, Wiesbaden, S. 25 bis 37.

Neckel, P.; Knobloch B. (2005): Customer Relationship Analytics: Praktische Anwendung des Data Mining im CRM, Heidelberg.

Paul, S. (2015): Angriff ist die beste Verteidigung: Banken brauchen Offensivspiel statt Abwehrschlacht, in: Börsen-Zeitung, Nr. 120, vom 27.6.2015, S. B3.

Peters, A.; Seitz, K. (2011): Die Vertriebspotenziale ausschöpfen: Cross Selling via Internet, in: BIT Banking and Information Technology, 12. Jg., Nr. 1, S. 32 bis 36.

Plath, K.-U. (2016): BDSG/DSGVO: Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. Aufl., Köln.

Sunikka, A.; Bragge, J. (2009): Promotional messages in multichannel banking: Attractive or annoying?, in: Journal of Financial Services Marketing, 14. Jg., Nr. 3, S. 245 bis 263.

Tinnefeld, M.-T.; Buchner, B.; Petri, T. (2012): Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht, 5. Auflage, München.

Ulbricht, C. (2016): Social Media und Recht: Praxiswissen für Unternehmen, 3. Auflage, Freiburg.

Wittmann, G.; Drexler, C.; Breitschaft, M.; Krabichler, T.; Stahl, E. (2007): Cross Selling bei Banken und Sparkassen: Empirische Analyse zu Status quo, Trends und zukünftigen Anforderungen, ibi research an der Universität Regensburg, ibi-Studie S 7101, Regensburg.

Zerfaß, K. (2016): Möglichkeiten der Ausgestaltung eines bankbetrieblichen Produktportfolios aus Sicht einer Universalbank, in: Hellenkamp, D.; Fürderer, K. (Hrsg.): Handbuch Bankvertrieb: Theorie und Praxis im Zukunftsdialog, Wiesbaden, S. 189 bis 208.

Fußnoten

1) Dapp 2014; Dapp 2015; Paul 2015.
2) Sunikka/Bragge 2009; Bragge/Sunikka/Kallio 2012.
3) Geenen/Dorschel/Dorschel 2015, S. 138.
4) Lieberknecht 2016, S. 35.
5) Lieberknecht 2016, S. 35; Zerfaß 2016, S. 191.
6) Zerfaß 2016, S. 204.
7) Wittmann et al. 2007; Peters/Seitz 2011.
8) Leonhardt 2017, S. 84 ff.
9) Gorgoglione/Panniello 2011; Leonhardt 2017.
10) Leußer/Hippner/Wilde 2011, S. 738 ff.; Leonhardt 2017, S. 45 ff.
11) Kerner 2002, S. 336; Neckel/Knobloch 2005, S. 57 f.; Gorgoglione/Panniello 2011, S. 91.
12) Bunzel/Gaess 2013, S. 41 f.
13) Cranor 2004, S. 63 ff.; Leonhardt 2017, S. 231.
14) Cranor 2004, S. 64.
15) Cranor 2004, S. 68 ff.
16) Cranor 2004, S. 58 f.
17) Tinnefeld/Buchner/Petri 2012, S. 212 und S. 221 f.
18) Tinnefeld/Buchner/Petri 2012, S. 221; Leonhardt 2017, S. 69 ff.
19) Heckmann in: Heckmann 2014, TMG, § 14, Rn. 321 ff.
20) Culmsee 2015, S. 168.
21) Plath in: Plath 2016, BDSG, § 28 BDSG, Rn. 101.
22) Köhler in: Köhler/Bornkamm 2016, UWG, § 7, Rn. 196; Ulbricht 2016, S. 262 f.
23) Lang 2013, S. 65.
24) Arndt 2011, S. 190; Eckhardt 2015, S. 276; Leonhardt 2017, S. 227.
25) Plath in: Plath 2016, BDSG, § 28 BDSG, Rn. 56 und Rn. 101.
26) Lang 2013, S. 52 f.
27) Leonhardt 2017, S. 228.
28) Leonhardt 2017, S. 232 f.
29) Kumar/Zhang/Luo 2014, S. 403 f.
30) Godin 1999, S. 43.
31) Leonhardt 2017, S. 232.
32) Cranor 2004, S. 70.