Die DSGVO im digitalen Bankgeschäft

Von David Klein

Quelle: pixabay

Im digitalen Bankgeschäft ist die Datenschutz-Grundverordnung eine Herausforderung. Das beginnt mit der Identifizierung der Kunden und möglichen Datenauslagerungen in eine Cloud. Noch heikler wird es beim Thema Big Data, das oft mit einer Änderung des ursprünglichen Zwecks der Datenverarbeitung einhergeht. David Klein empfiehlt deshalb die Anonymisierung personenbezogener Daten. Denn Datenschutzverstöße können auch leicht die BaFin auf den Plan rufen. Red.

Banken galten in der öffentlichen Wahrnehmung lange als wahre Trutzburgen des Datenschutzes, wenn man so will: Das Bankgeheimnis, das eine Weitergabe von Informationen über Kunden und Vermögensverhältnisse an Dritte quasi unmöglich machte, hatte den Ruf unerschütterlich zu sein. Doch die digitale Welt tickt anders – getreu dem Motto „panta rhei" fristen Daten nicht länger ein Schicksal in Schließfächern, sondern sollen vielmehr im größtmöglichen Maße genutzt werden.

Den Ruf der digitalen Wirtschaft hat die ganze Finanzbranche mehr als deutlich vernommen. Die Schlagworte Banking as a Platform (BaaP), Robo Advisory und Blockchains finden sich in den Digitalstrategien von Banken wieder.

Mehr als 150 Millionen Giro- und Onlinekonten[1)] führen die deutschen Banken. Zum Vergleich: Der E-Commerce-Riese Amazon hatte 2016 „nur" rund 17 Millionen zahlende Prime-Kunden. Die Banken horten damit einen großen Schatz von Informationen über ihre Kunden, von denen ein – wenn auch großer – Online-Händler nur träumen kann. Jeder Bankkunde verrät seiner Bank zum Beispiel eine Menge über sein Einkaufsverhalten, und zwar nicht nur bei einem Online-Händler, sondern bei allen, bei denen er im Idealfall seine Bankkreditkarte zum Bezahlen einsetzt. Und nicht nur das: Daneben erfährt die Bank auch, über welches Einkommen der Kunde verfügt, wo er wohnt und vieles mehr.

Datenschätze bei der Bank

Die Bank führt eine Vielzahl von Daten zusammen, die normalerweise in Silos voneinander getrennt bei verschiedenen Stellen verwahrt werden. Diese sehr konkreten Daten können dann wertvoll sein, wenn hieraus Informationen abgeleitet werden können, die den Kunden entweder dazu bewegen, eigene Produkte der Bank oder Drittprodukte anderer Unternehmen zu erwerben.

Zum Autor

Dr. David Klein, Fachanwalt für Informationstechnologie, Taylor Wessing Partnerschaftsgesellschaft mbB, Hamburg

Die Frage, die sich in diesem Zusammenhang nicht erst seit dem 25. Mai 2018 nach Geltung der europaweit einheitlichen Datenschutz-Grundverordnung[2)] stellt, ist nur, ob diese Daten überhaupt wertschöpfend genutzt werden können.

Die Grundlage: Infrastruktur digitalisieren

Doch eins nach dem anderen: Zu Beginn einer Datennutzungsstrategie muss die Infrastruktur der Bank erst einmal digital werden. Was profan klingt, bedeutet einen erheblichen technischen und prozessualen Aufwand. Alte Kernbankensysteme können den Schritt in die Digitalisierung oft nicht mitgehen und müssen ersetzt werden. Und für die Umsetzung einer sinnvollen Banking-as-a-Platform-Strategie bleibt eigentlich nur die Cloud. Doch Cloud und Bank, passt das überhaupt?

Der Schritt in die Cloud ist nicht mehr und nicht weniger als eine Auslagerung im bankenaufsichtsrechtlichen Sinn. Die Vorgaben aus dem Kreditwesengesetz und die dazugehörige Konkretisierung in den BAIT[3)] an die Sicherheit und Auditierbarkeit müssen daher eingehalten werden. Somit scheiden etwa Cloud-Dienstleister aus, die sich weigern, mit der BaFin als zuständige Aufsichtsbehörde für deutsche Kreditin-

stitute zusammenzuarbeiten. Gerade bei der weiteren Auslagerung darf die Bank daher nicht die Augen vor möglichen Konflikten schließen.

DSGVO bestimmt Vertragswerk für die Auslagerung in die Cloud

Im Rahmen der Wahl einer Cloudlösung muss andererseits nicht immer auf externe Lösungen zurückgegriffen werden. Sogenannte private Clouds, also Cloud-Lösungen, die bei der Bank selbst betrieben werden, gelten natürlich nicht als Auslagerung. Allerdings kann und will nicht jede Bank auf eine interne Lösung zurückgreifen, die im Zweifel unter den Gesichtspunkten Verfügbarkeit und Skalierbarkeit ohnehin keine Alternative darstellt.

Bei der Auslagerung spielt dann das erste Mal die Datenschutz-Grundverordnung eine Rolle: Sie diktiert, welche Anforderungen an den Datenschutz in der Cloud bestehen und welches Vertragswerk für die Auslagerung erforderlich ist.

Digitalisierung des Kunden: Privacy bei Design für Identifizierungsdienste

Mit der digitalen Infrastruktur ist die Bank noch lange nicht digital. Sondern Digitalisierung bedeutet bei Banken nicht zuletzt auch, Service, Beratung und Produkte zu digitalisieren. Was mit dem Telefonbanking begann, ist nun als Online-Banking oder Mobile-Banking für viele Kunden eine Selbstverständlichkeit und sie besuchen ihre Bankfiliale ausschließlich online.

Die Bank muss hierbei sicherstellen, ihre Kunden noch zu kennen: Die Kundenidentifizierung online geht etwas anders vonstatten als die Identifizierung beim Kundenberater, den der Kunde seit Kindesbeinen persönlich kennt. Identifikationsdienste können mittlerweile in wenigen Minuten mit dem Kunden zusammen die Identifizierung vornehmen, ohne dass der Kunde das Haus verlassen muss: Ein Smartphone und der Personalausweis genügen hierfür.

Viele Identifizierungsdienste sind sich ihrer besonderen Verantwortung bewusst und berücksichtigen deshalb bei der Struktur ihrer Dienste datenschutzrechtliche Grundsätze der Transparenz und des sogenannten „privacy by design" bereits: Das ist die Grundvoraussetzung für die datenschutzkonforme Ein- und Anbindung solcher Dienste an die eigene Bankeninfrastruktur.

Die Digitalisierung der Bankprodukte und -dienstleistungen ermöglicht die Datensammlung, die wiederum Ausgangsbasis für die Auswertung und Analyse für die Optimierung der Bank ist. Allerdings ist die Datennutzung nicht schrankenlos möglich, ganz im Gegenteil. Die Kenntnis der datenschutzrechtlichen und bankaufsichtsrechtlichen Grenzen der Datenverarbeitung ist entscheidend für die spätere Nutzbarkeit der Daten und für die Architektur der IT-Systeme, die für die Datensammlung genutzt werden. Dies wird im Folgenden deutlich.

Einwilligung ist nicht gleich Einwilligung

Die Nutzbarkeit von Transaktionsdaten, also der Daten, die ein Zahlungsdienstleister (etwa eine Bank) vom Zahlungsdienstnutzer (dem Kunden) verarbeitet, wenn dieser eine Zahlung beauftragt, ist augenscheinlich Gegenstand sowohl der bankenaufsichtsrechtlichen Regelungen als auch des Datenschutzes in der Datenschutz-Grundverordnung.

Bankenaufsichtsrechtlich geben die Art. 94 (2) der PSD2[4] beziehungsweise die Umsetzung in § 59 (2) ZAG[5] vor, die für die Erbringung der Zahlungsdienstleistung notwendigen personenbezogenen Daten des Nutzers nur mit der ausdrücklichen Zustimmung beziehungsweise Einwilligung des Nutzers zu verarbeiten.

Datenschutzrechtlich kennt die Datenschutz-Grundverordnung neben einer Einwilligung allerdings weitere Rechtsgrundlagen, um personenbezogene Daten zu verarbeiten: etwa die Daten, die für die Eingehung oder Durchführung eines Vertragsverhältnisses erforderlich sind, oder wenn ein berechtigtes Interesse des Verantwortlichen für die Datenverarbeitung besteht. Oder anders ausgedrückt: Eine Einwilligung, die im Zweifel mühsam eingeholt werden muss und eine Aktion des Kunden verlangt, ist unter dem Gesichtspunkt der „customer experience" unter Umständen gar nicht wünschenswert.

Widerspruch zwischen Bankaufsichts- und Datenschutzrecht?

Der scheinbare Widerspruch zwischen Bankaufsichtsrecht und Datenschutzrecht hat eine einfache Ursache: Der Gesetzgeber hört sich selbst nicht zu. PSD2 und Datenschutz-Grundverordnung sind nebeneinander entstanden. Statt frühzeitig die Expertise etwa der europäischen Datenschutzaufsichtsbehörden, gebündelt in der sogenannten Art. 29 Working Party (WP) beziehungsweise heute des European Data Protection Boards (EDPB), mit einzubeziehen, blieben diese außen vor.

Der vermeintliche Konflikt der Regelungen und damit eine Unsicherheit, wie und in welchem Umfang die Transaktionsdaten verwendet werden dürfen, ist durch das EDPB gelöst worden. Das EDPB stellte klar, dass selbstverständlich die Datenschutz-Grundverordnung den Takt in Europa für die Verarbeitung von personenbezogenen Daten vorgibt. Daran ändert auch die scheinbar widersprüchliche und stark limitierende Regelung in der PSD2 nichts.

Kein Freibrief für Datenauswertungen

Für die Verarbeitung der Transaktionsdaten braucht es daher keiner ausdrücklichen datenschutzrechtlichen Einwilligung, ein Freibrief für die spätere Nutzung für Aus-

wertungen und Analysen zu Marketingzwecken bedeutet dies allerdings nicht.[6)] Die weitere Nutzung der Transaktionsdaten für andere Zwecke als die Durchführung der Zahlung (sowohl des Nutzers als auch der „silent party", also etwa der an der Transaktion als Empfänger Beteiligten) ist allerdings nach Ansicht des EDPB nur mit der ausdrücklichen datenschutzrechtlichen Einwilligung möglich.[7)]

Diese weitere Nutzung betrifft etwa die Analyse von Kaufgewohnheiten, um den Bedarf an Verbraucherkrediten zu präzisieren, oder auch die Möglichkeit, Fremdprodukte wie Versicherungsleistungen anzubieten, wenn entsprechender Sepa-Zahlungsverkehr Lücken in der Abdeckung mit solchen Leistungen offenbart.

Die Gestaltung von Einwilligungen kann auf verschiedene Art und Weise erfolgen. Sinnvoll erscheint aber, dem Kunden seine in der Datenschutz-Grundverordnung manifestierte Datensouveränität zu lassen und ihm direkt an der Quelle der Daten ein Einwilligungsinstrument an die Hand zu geben, etwa durch Auswahl der Kontoinformationsdienste, die Zugriff auf Kontodaten erhalten dürfen, und den Umfang der Zugriffsbefugnisse sowie der jeweiligen Zwecke.

Big Data & Co.

Darauf aufbauend stellt sich die Frage: Nutze ich ausschließlich eigene Daten oder versuche ich, diese Daten aus anderen Quellen zu erhalten? Gerade unter dem Schlagwort „Big Data" tritt oftmals eine Vermengung dieser Daten ein. Der besondere Reiz bei Big Data liegt in der Auswertung und Nutzung einer großen Menge Daten aus unterschiedlichsten Quellen für neue Erkenntnisse, die das eigene Geschäftsmodell voranbringen können oder eine erleichterte Vermarktung von eigenen und fremden Produkten ermöglichen.

Diese Situationen kennen die Banken teilweise schon, sind sie doch gesetzlich etwa dazu verpflichtet, bei der Vergabe von Krediten ein Kreditscoring durchzuführen, das etwa die wirtschaftliche Leistungsfähigkeit des Antragstellers prüft. Hierbei wird auf Daten zurückgegriffen, die nicht nur die Bedienung von Krediten der kreditgebenden Bank aus der Vergangenheit wiederspiegeln, sondern vielmehr mit unzähligen Daten etwa aus dem Konsumverhalten der Person angereichert sind. Nur so kann ein Gesamtbild entstehen, das eine verlässliche Prognose für das Risikomanagement der Bank zulässt.

Daten aus Suchverläufen oder sozialen Netzwerken können die Genauigkeit der Vorhersage im Rahmen des Scorings deutlich erhöhen. Ähnliches gilt auch für die Fraud Prevention beim Einsatz von bargeldlosen Zahlungsmitteln: Kann ich die Daten des jeweils Betroffenen zu Reisebuchungen auswerten, kann der Herausgeber der Kreditkarte umgehend prüfen, ob Auslandseinsätze durch den Kunden vorgenommen wurden oder möglicherweise der Verdacht einer entsprechenden ungenehmigten Transaktion besteht.

Die im Rahmen der Vertragsbeziehung mit dem Kunden gewonnenen Daten können mit weiteren Daten angereichert werden, um dem Bankkunden ganz gezielt passgenau Vorschläge für weitere Produkte anzubieten. So könnte etwa aufgrund der Auswertung von weiteren Daten darauf geschlossen werden, ob beziehungsweise wann ein Bankkunde die nächste größere Anschaffung plant. Hierzu könnte die Bank dann wiederum einen maßgeschneiderten Kredit anbieten, der das Konsumverhalten unterstützt, und dem Kunden den Kredit zu besseren als den üblichen Konditionen gewähren.

Grenzen der Datenverwertbarkeit

Gerade im Bereich Big Data, also der Zusammenführung von Daten aus unterschiedlichsten Quellen und von unterschiedlichster Datenqualität und Datenart, setzen zum einen die Regulierung und zum anderen der Datenschutz Grenzen in Bezug auf die Verwertbarkeit echter, personenbezogener Daten. Andererseits haben die Bankenaufsichten in Deutschland[8)] und Europa[9)] das große Potenzial von Big-Data-Anwendungen realisiert. So könnte Big Data nicht nur bei der Kundengewinnung eingesetzt werden, sondern vor allem im Bereich IT-Sicherheit, zur Verbesserung von Identifikationsprozessen aber auch zur Auswertung des Ausgabeverhaltens.

Das Datenschutzrecht sieht in einer Big-Data-Auswertung personenbezogener Daten in der Regel eine Änderung des ursprünglichen Zwecks der Verarbeitung. So können zum Beispiel Daten, die ursprünglich von einem Betroffenen in einem sozialen Netzwerk veröffentlicht wurden, später für einen ganz anderen Zweck, etwa zur Verbesserung des Kreditscorings genutzt werden. Es ist offensichtlich, dass die beiden Zwecke nicht deckungsgleich sind sondern der Zweck sich nachträglich ändert.

Die Zweckänderung muss nach der Datenschutz-Grundverordnung besondere Voraussetzungen erfüllen, damit sie zulässig ist und nicht etwa einer weiteren Einwilligung bedarf. Wesentlich ist die Vereinbarkeit des ursprünglichen Zwecks der Datenverarbeitung mit dem geänderten, neuen Zweck: Konnte der Kunde zum Beispiel erwarten, dass seine Daten für diese anderen Zwecke verwendet werden? Je transparenter die möglicherweise auch anderweitige Nutzung der Daten gegenüber dem Kunden kommuniziert wird, desto eher kann er eine weitere Verarbeitung erwarten.

Naheliegende Lösung: Anonymisierung personenbezogener Daten

Die Festlegung des EDPB auf die eher eingeschränkte Nutzbarkeit personenbezogener Daten Dritter im Zusammenhang mit Kontoinformationsdiensten[10)] lässt allerdings bereits erahnen, dass eine umfassende Datenverarbeitung oder eine Datenverarbeitung zu anderen als den ursprünglichen Zwecken herausfordernd

werden kann. Außerdem sprechen die Grundsätze der „Datenminimierung" und „Speicherbegrenzung" in Art. 5 der Datenschutz-Grundverordnung eher gegen ungezügelte Big Data Anwendungen.

Die naheliegende Lösung gerade im Bereich des echten Big Data ist daher die Anonymisierung personenbezogener Daten, um diese nach der Anonymisierung frei von den Zwängen des Datenschutzrechtes weiter verarbeiten zu können.

Auch wenn nicht für jede Big-Data-Anwendung ein Arbeiten auf solchen anonymisierten Daten möglich ist und zudem die latente Gefahr besteht, dass selbst eine Anonymisierung von Daten im Laufe der Verarbeitung aufgehoben wird und aufgrund der Vielzahl der gewonnenen Daten und Erkenntnisse einer Identifizierung einer natürlichen Person wieder möglich ist, ist datenschutzrechtlich eine Anonymisierung empfehlenswert. Mit diesen anonymisierten Daten können etwa präzise statistische Modelle erstellt werden, die dann wiederum als „Blaupause" genutzt werden können. Gerade im Bereich des Risikomanagements aber auch des Direktmarketings und des predictive Targetings sind anonymisierte Datenmodelle aus Sicht des Datenschutzes vorzugswürdig.

Datenschutzverstöße können die BaFin auf den Plan rufen

Auf der bankenaufsichtsrechtlichen Seite darf eine Big-Data-Anwendung nicht dazu führen, eine „Black Box" für Entscheidungsprozesse zu schaffen. Gerade in Kombination mit künstlicher Intelligenz müssen Entscheidungsprozesse transparent und auditierbar bleiben, damit das Vertrauen der Kunden in die Bank nicht zerstört wird.

Zugleich können Datenschutzverstöße unter Umständen Zweifel an der Zuverlässigkeit der Geschäftsführung aufkommen lassen. Das bedeutet, dass eine datenschutzrechtliche Untersagungsverfügung einer Datenschutzaufsichtsbehörde oder im schlimmsten Falle sogar die Verhängung eines Bußgeldes gleichzeitig die BaFin auf den Plan rufen kann, zu prüfen, ob die Verlässlichkeitskriterien der Geschäftsführung noch erfüllt werden.

Die Nutzung personenbezogener Daten für Marketing- und Analysezwecke im Bereich der Kreditwirtschaft bedürfen einer sorgfältigen rechtlichen und strukturellen Planung. Dann allerdings können datenschutzkonform und im Einklang mit dem Bankenaufsichtsrecht Big Data & Co. gewinnbringend genutzt werden.

Fußnoten:
1) Quelle: Deutsche Bundesbank, Stand 27. Oktober 2017.
2) Verordnung (EU) 2016/679.
3) Bundesanstalt für Finanzdienstleistungsaufsicht, Rundschreiben 10/2017 (BA) - Bankaufsichtliche Anforderungen an die IT (BAIT), 6. November.2017.
4) Richtlinie (EU) 2015/2366, Payment Services Directive 2.
5) Gesetz über die Beaufsichtigung von Zahlungsdiensten.
6) Vgl. EDPB, Letter 5 July 2018, S. 4.
7) aaO.
8) BaFin Studie „Big Data trifft auf künstliche Intelligenz - Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen", 15. Juni 2018.
9) So bereits 2016 die Europäische Bankenaufsicht EBA/DP/2016/01 vom 4. Mai 2016.
10) EDPB, Letter 5 July 2018, S. 3.