Swiss Banking

Umgang mit Daten im Geschäftsalltag

Mai 2021

Leitfaden der SBVg

	Executive Summary	**3**
1	**Einleitung**	**4**
2	**Regelungskonzepte der Datenbearbeitung**	**6**
	2.1 Grundlagen für den richtigen Umgang mit Daten	6
	2.2 Profiling	9
	2.3 Rechtfertigungsformen	9
	2.4 Technische und organisatorische Massnahmen (TOM)	11
	2.5 KI – Governance	13
3	**Anwendungsfälle**	**16**
	3.1 Nutzung von künstlicher Intelligenz für Compliance-Zwecke	16
	3.2 Kreditprüfung	17
	3.3 Trendanalysen und Benchmarking	19
	3.4 Biometrische Authentifizierung	21
	3.5 Personalisierte Angebote und Beratung	23
	3.6 Loyalitätsprogramme	26

Executive Summary

Dieser Leitfaden veranschaulicht allgemeine Regelungskonzepte zur Datenbearbeitung anhand von sechs unterschiedlichen Anwendungsfällen aus dem Bankgeschäft. Im Zentrum stehen Grundlagen rund um das revidierte Datenschutzgesetz, der Umgang mit Rechtfertigungsformen, technische und organisatorische Massnahmen (TOM) sowie Massnahmen rund um die Anwendung Künstlicher Intelligenz (KI), insbesondere bei der automatisierten Bearbeitung von Personendaten. Der Leitfaden richtet sich in erster Linie an die Mitglieder der SBVg und soll eine Orientierungshilfe bieten, um die Opportunitäten, welche die Datennutzung bietet, auf eine sichere Art und Weise ergreifen zu können.

- **Einsatz von KI für Compliance-Zwecke:** Die Bank muss das mit dem Einsatz von KI verbundene Risiko einschätzen und sollte ein entsprechendes Einsatzkonzept erstellen. Insbesondere gilt es, angemessene TOM zu dokumentieren. Bei der Wahl der TOM ist auf die Einhaltung der datenschutzrechtlichen Bearbeitungsgrundsätze zu achten.
- **Kreditprüfung:** Die Qualität der verwendeten Daten sollte jederzeit abschliessend, einwandfrei und deren Herkunft klar ersichtlich sein. Damit nur qualitativ einwandfreie Daten verwendet werden, bietet es sich aus datenschutzrechtlicher Sicht an, bei Zweifeln an der Herkunft der Daten oder fehlenden Verifizierungsmöglichkeiten, auf eine Bearbeitung dieser Daten zu verzichten.
- **Trendanalysen und Benchmarking:** Die Anonymisierung von Personendaten birgt das Restrisiko der Re-Identifikation. Hier soll mittels angemessener TOM sichergestellt werden, dass eine Re-Identifizierung nicht möglich ist. Analysen sollten so gestaltet werden, dass bei Bedarf nachvollziehbare Erläuterungen über die Zusammensetzung der Datensätze und verwendete Verarbeitungsmethoden gegeben werden können.
- **Biometrische Authentifizierung:** Hinsichtlich der Beurteilung der Angemessenheit der TOM, z.B. bezüglich der Datenspeicherung, sind biometrische Daten als besonders schützenswerte Personendaten angemessen zu berücksichtigen. Eine transparente Kommunikation betreffend Einsatz von biometrischen Erkennungssystemen kann die Hemmschwelle zur kundenseitigen Nutzung senken.
- **Personalisierte Angebote und Beratung:** Die Datenanalyse zu diesem Zweck ist bei Vorliegen der Grundanforderungen und in Anwendung des Grundsatzes von Treu und Glauben immer ohne Weiteres zulässig, wenn die Analyse auf Daten basiert, welche der Kunde selbst der Bank zur Verfügung gestellt hat und die Daten von der Bank in Zusammenhang mit ihrer typischen Banktätigkeit erhoben wurden.
- **Loyalitätsprogramme:** Standardisierte Kundenbindung ist aus einer Datenschutzperspektive unproblematisch. Bei individualisierten Programmen besteht insbesondere eine Informationspflicht. Kunden sollen darauf hingewiesen und informiert werden, bevor sie in solche Programme eingebunden werden. Die Informationspflicht kann entfallen, wenn der Kunde bereits bei der Geschäftseröffnung informiert wurde.

1 Einleitung

Die Nutzung von Daten wird für die Finanzbranche von immer grösserer Bedeutung. Die Art und Weise, wie Daten genutzt werden können, dürfen und sollen, wird sich in den nächsten Jahren – getrieben durch technologische Entwicklungen, veränderte Kundenbedürfnisse und regulatorische Anforderungen – weiter stark verändern. Eine effiziente Nutzung von Daten ermöglicht es den Finanzinstituten, personalisierte und damit relevantere Angebote und Dienstleistungen zu offerieren. Dies führt letztlich zu einer besseren Beratung des Bankkunden[1]. Zudem führt eine optimale Datennutzung zu effizienteren Prozessen, niedrigeren Kosten und einem verbesserten Risikomanagement. Tatsache ist: Integrität und Kundenvertrauen haben für Schweizer Banken immer oberste Priorität. Dies bedeutet vor allem Transparenz im Hinblick auf die Datenbearbeitung und deren Zweck. Es ist zentral, dass die Finanzbranche bei Fragestellungen zu einem verantwortungsvollen Umgang mit Daten neben regulatorischen und technischen Aspekten (wie z.B. der Datensicherheit) auch die Kundenperspektive bzw. die Erwartungen der Kunden berücksichtigt.

Mit diesem Ziel – und vor dem Hintergrund der Einführung des neuen Datenschutzgesetzes (revDSG) – hat eine Arbeitsgruppe unter der Leitung der Schweizerischen Bankiervereinigung (SBVg) diesen Leitfaden erstellt. Er beleuchtet sechs unterschiedliche Anwendungsfälle von Datenbearbeitungen in der Praxis und soll die Mitglieder der SBVg im alltäglichen Umgang mit Daten unterstützen. Er ist weder ein juristisches noch ethisches Grundsatzpapier. Vielmehr werden darin exemplarisch Anwendungsfälle dargestellt, die im Bankalltag bereits heute eine grosse Rolle spielen. Dadurch unterscheidet er sich von anderen Publikationen, bei denen ein ganzheitlicher Ansatz gewählt oder umfassende Verhaltensregeln (Code of Conduct) für eine Branche festgelegt werden. Der Leitfaden definiert keine branchenweiten Mindeststandards. Des Weiteren erhebt er keinen Anspruch auf Vollständigkeit und wird nach Bedarf periodisch aktualisiert und erweitert. Es bleibt jedem einzelnen Finanzinstitut überlassen, die Inhalte dieses Dokuments im Rahmen der institutsspezifischen Risikobeurteilung zu interpretieren bzw. anzuwenden.

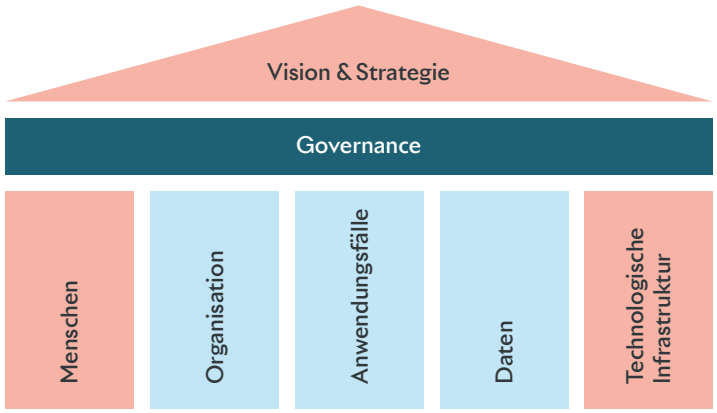
Aufbau des Leitfadens

Worauf im Umgang mit Daten im Geschäftsalltag geachtet werden soll, wird im Folgenden anhand eines «Frameworks» (siehe Abb. 1) dargestellt. Neben der Organisation, den Daten und Anwendungsfällen, auf die in diesem Leitfaden fokussiert wird, spielen auch die Vision und Strategie eines Unternehmens, der Umgang mit Mitarbeitenden, Fragen der Kultur und Details rund um die technologische Infrastruktur eine zentrale Rolle. Da dies jedoch höchst individuelle Bereiche sind, welche am besten auf Institutsebene angegangen werden, behandelt sie dieser Leitfaden nicht oder nur am Rand.

1 Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Publikation die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Abbildung 1

Framework der zu beachtenden Faktoren beim Umgang mit Daten



Quelle: SBVg

Bei der Auswahl der diskutierten Anwendungsfälle wird in erster Linie auf eine breite Abdeckung des Bankgeschäfts abgezielt. Je nach Fall kann eine effektive und zielgerichtete Datennutzung entweder bei bestehenden Kundendienstleistungen, der Erschliessung von neuen Kundendienstleistungen oder bei der Risikominderung unterstützen. Die mit den Anwendungsfällen verbundenen Risiken [2] sind je nach Art, Menge und Bearbeitungsform von Daten unterschiedlich zu bewerten. Diese Risikoeinschätzung ist im Rahmen der bankinternen Governance vorzunehmen und die daraus folgenden geschäftspolitischen Entscheidungen sind mit Blick auf die Einhaltung der datenschutzrechtlichen Grundsätze wie Zweckbindung, Transparenz, Rechtmässigkeit und Verhältnismässigkeit (z.B. mit der Ausprägung Datensparsamkeit) zu treffen. Vorgaben zu technischen und organisatorischen Massnahmen (sog. TOM-Vorgaben) unterstützen die richtige und effiziente Umsetzung der rechtlichen Anforderungen (vgl. Kapitel 2.4).

Auch das Verhältnis zwischen der Bank und ihren Kunden ist zu berücksichtigen. In diesem Zusammenhang können die verschiedenen Kundeninformationsformen vertrauensbildend eingesetzt werden. Es ist dabei für jeden Anwendungsfall zu beurteilen, ob eine Diskrepanz zwischen den Erwartungen der Kunden und den tatsächlichen Aktivitäten der Bank vorliegt. Diese gilt es zu beseitigen, ggf. mit einer Datenschutzerklärung oder weiteren Transparenzmassnahmen. Die konkrete Ausgestaltung der Governance ist von Grösse, Struktur, Komplexität, Geschäftsmodell und Risiken der jeweiligen Bank abhängig. Für die einzelnen Anwendungsfälle wird eine solche Governance vorausgesetzt. Die darüber hinaus notwendigen Detailausprägungen werden jeweils wie folgt dargestellt:

a. **Hintergrund:** Einführung ins Thema und den Mehrwert für Kunden und Banken;
b. **Anwendungsmöglichkeiten:** Skizzierung verschiedener Beispiele;
c. **Mögliche Fragestellungen:** Relevante Fragestellungen mit möglichen Lösungsansätzen.

2 Risiken können u.a. rechtlicher, reputationsmässiger oder operativer Natur sein.

2 Regelungskonzepte der Datenbearbeitung

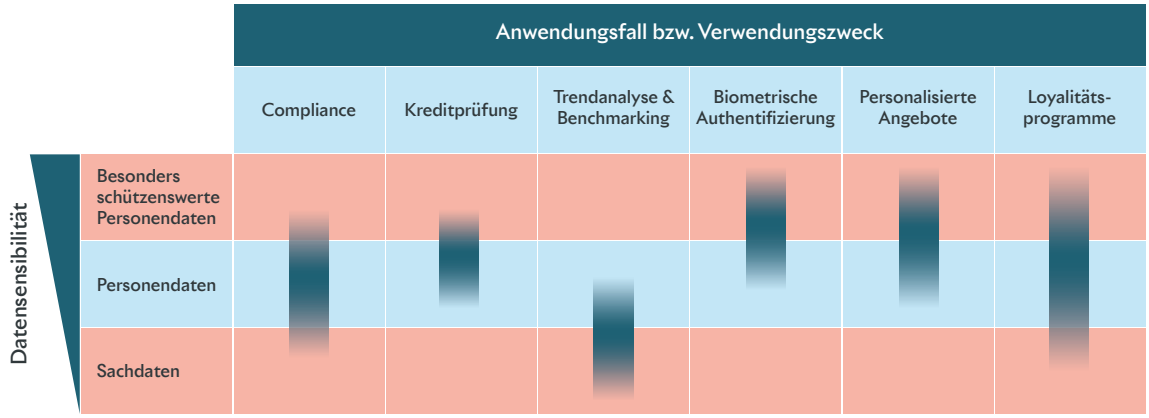
2.1 Grundlagen für den richtigen Umgang mit Daten

Unabhängig davon, welche Art von Daten bearbeitet wird, muss der jeweilige Verwendungszusammenhang stets berücksichtigt werden. Sowohl das bestehende als auch das revidierte DSG ermöglichen die Klassifizierung von Daten entlang folgender grober Unterteilung:

1. **Sachdaten**[3] **(nicht explizit im revDSG erwähnt):** Daten, die mangels Personenbezug keine Rückschlüsse auf Individuen ermöglichen, sind keine Personendaten. Dazu gehören auch anonymisierte Daten. Solche Daten sind sachlogisch nicht vom revDSG erfasst.
2. **Personendaten (Art. 5 lit. a revDSG):** Dazu zählen sämtliche Daten die, zum Beispiel auch in Kombination und Korrelation mit anderen Daten, einen Personenbezug aufweisen. Dies können einerseits statische Daten sein, aber auch Daten, welche Rückschlüsse auf das Verhalten einer Person zulassen, beispielsweise Transaktionsdaten oder Geodaten.
3. **Besonders schützenswerte Personendaten (Art. 5 lit. c revDSG):** Ein durch den Gesetzgeber abstrakt und abschliessend definierter Katalog von Personendaten. Zum Beispiel biometrische oder religiöse und weltanschauliche Daten, aber auch Informationen zur Intimsphäre oder zur Gesundheit[4].

Abbildung 2

Einschätzung des Datenverwendungszwecks und der damit einhergehenden Datensensibilität



Quelle: SBVg

3 Die EU-Kommission spricht in diesem Zusammenhang auch von «nicht-personenbezogenen Daten».

4 Vgl. vollständigen Katalog in Art. 5 revDSG.

Durch diese Dreiteilung von Sachdaten, Personendaten und besonders schützenswerten Personendaten lassen sich die gewählten Anwendungsfälle schematisch anhand ihrer jeweiligen Sensibilität einordnen. Der Leitfaden wird in der Folge zeigen, dass die rechtliche Abgrenzung nicht immer eindeutig ist.

Die aufgeführte Datensensibilität leitet sich aus dem Datenschutzrecht ab und muss nicht in jedem Fall identisch mit der subjektiven, vom Kunden wahrgenommenen Sensibilität sein. Auch innerhalb derselben Datenkategorie kann es sinnvoll sein, den konkreten Lösungsansatz entsprechend der subjektiven Datensensibilität und der damit einhergehenden Risikolage unterschiedlich streng auszugestalten. Im Umgang mit Personendaten von Bankkunden, sogenannten «Client Identifying Data» (CID)[5], gilt zusätzlich zu den datenschutzrechtlichen Grundsätzen das Bankkundengeheimnis nach Art. 47 Bankengesetz (BankG)[6], welches die strafrechtliche Verstärkung der zivilrechtlich begründeten Geheimhaltungspflichten ist. Vor diesem Hintergrund hat die Eidgenössische Finanzmarktaufsicht FINMA bestimmte technische und organisatorische Anforderungen bezüglich des Umgangs mit elektronischen Kundendaten festgelegt[7]. Die Darstellung der betroffenen Datenkategorien in Abbildung 2 ist nicht abschliessend zu verstehen, sondern dient lediglich der visuellen Groborientierung der Anwendungsfälle in Abschnitt 3. Der Begriff «Datensensibilität» wurde bewusst offen gewählt und soll Reputationsrisiken, Kunden- und öffentliche Wahrnehmung, sowie ethische Fragestellungen adressieren. Tatsächlich bildet jede individuelle Risikoeinschätzung einer Bank auch immer den institutsspezifischen Risikoappetit ab und kann daher variieren.

Privacy Icons

Bearbeitungen von Personendaten müssen für die betroffene Person erkennbar sein. Normalerweise wird zur Kenntlichmachung gegenüber dem Kunden das Instrument der Datenschutzerklärung herbeigezogen. In der Praxis kann aber davon ausgegangen werden, dass diese Texte nicht oder nur oberflächlich gelesen werden. Um die Bearbeitung von Daten transparenter zu gestalten bieten sich Piktogramme an. Eine kostenlose und einfach zu lizensierende Lösung bietet der Verein Privacy Icons (🔗 www.privacy-icons.ch/) an. Diverse Schweizer Unternehmen aus verschiedenen Branchen haben diese oder ähnliche Lösungen bereits implementiert.

5 CID ist eine Definition der FINMA, die Personendaten natürlicher Personen und den ihnen zugehörigen Domizilgesellschaften, Trusts etc. umfasst. Zusammen werden diese als «Privatkunden» bezeichnet.

6 Daten von juristischen Personen und anderen Unternehmen und damit auch Domizilgesellschaften und Trusts qualifizieren unter dem revDSG nicht mehr als Personendaten, soweit sie keinen Bezug zu einer natürlichen Person aufweisen. Daten von juristischen Personen (sowie auch von institutionellen Kunden) fallen aber grundsätzlich unter das Bankkundengeheimnis.

7 Vgl. namentlich Anhang 3 «Umgang mit elektronischen Kundendaten» des FINMA-RS 08/21 «Operationelle Risiken – Banken».

Open Banking bzw. Open Finance

Mit der zunehmenden Fragmentierung der Wertschöpfungskette werden Kunden vermehrt über eine Vielzahl unterschiedlicher Finanzdienstleister wie Banken, Versicherungen, Fin-Techs und branchenfremde Dienstleister bedient. Die SBVg hat diese Entwicklungen in einer dedizierten Auslegeordnung detailliert beleuchtet. Für den vorliegenden Leitfaden ist zentral, dass diese Vernetzung von Banken und externen Dienstleistern den Austausch von (Kunden)-Daten voraussetzt.

Für Open Banking bzw. Open Finance gibt es unterschiedliche Anwendungsmöglichkeiten, sowohl im Firmenkunden- wie auch im Privatkundensegment. Folgende Beispiele veranschaulichen mögliche Anwendungsfelder:

- **Verbesserte Liquiditätsplanung** für Geschäftskunden durch Einbindung in Buchhaltungssoftware.
- **Aggregierung der Finanzlage:** Transparenz über die eigene finanzielle Situation von Geschäfts- und Privatkunden durch Aggregierung verschiedener Konten und Vermögenswerte über einen Drittanbieter.
- **Zahlungen:** Einfachere, schnelle und sichere Transaktionen über einen externen Anbieter.

All diesen Anwendungsmöglichkeiten ist gemeinsam, dass Kundendaten zwischen Bank und Drittanbieter fliessen. Die Banken sehen sich beim Austausch von Kundendaten mit den Anforderungen des Datenschutzrechtes und des Bankkundengeheimnisses konfrontiert. Aus Kundensicht stellt sich die Frage, unter welchen Voraussetzungen eine Bank Kundendaten an externe Parteien weitergeben darf. Abhängig von der Art und Intensität der Zusammenarbeit zwischen Bank und Drittanbieter steigen jeweils auch die Prüf- und Sorgfaltspflichten der Bank gegenüber dem Drittanbieter.

Die Zusammenarbeit und der Datenfluss zwischen Kunde, Bank und Drittanbieter sind klar, gegebenenfalls vertraglich, zu dokumentieren. Zu berücksichtigen ist dabei die Möglichkeit, dass Open Banking bzw. Open Finance zwischen zwei (oder mehreren) Banken stattfinden kann. Schliesslich spielt die Transparenz gegenüber dem Kunden eine entscheidende Rolle. Kunden sollten darüber informiert sein, welche Daten mit Drittanbietern geteilt werden und was beim Drittanbieter mit deren Daten geschieht. Bei solchen Drittanbietern bzw. Geschäftspartnern einer Bank handelt es sich i.d.R. nicht um «echte Dritte» im Sinne des revDSG. Deshalb ist im Bereich von Open Banking bzw. Open Finance zur Datenübertragung durch die Bank auf solche Geschäftspartner typischerweise keine vorgängige Einwilligung des Kunden notwendig. Nur bei Übertragung von Daten auf «echte» Dritte stellt sich diese Frage und zwar aufgrund des Bankkundengeheimnisses (vgl. Kapitel 2.3).

https://www.swissbanking.ch/de/downloads

2.2 Profiling

Gemäss revDSG (Art. 5 lit. f und g) ist Profiling die automatisierte Bearbeitung von Personendaten, die der Bewertung bestimmter persönlicher Aspekte, wie Arbeitsleistung, wirtschaftlicher Verhältnisse, Gesundheit, Vorlieben, Aufenthaltsort oder Mobilität dient. Durch die Bearbeitung von Daten, insbesondere die Erstellung von Korrelationen von Daten, können bestimmte Merkmale und Verhaltensweisen von Personen oder Gruppen von Personen analysiert und mit einer gewissen Wahrscheinlichkeit vorausgesagt werden.

So kann zum Beispiel anhand der automatisierten Bearbeitung von Daten aus dem Zahlungsverkehr das individuelle Zahlungsverhalten ausgewertet werden, um mit Blick auf Betrugsprävention Anomalien bei den Zahlungsaufträgen sofort zu erkennen und zum Schutz des Kunden und der Bank entsprechende Zahlungsaufträge zu stoppen (vgl. Kapitel 3.1 u. 3.5). Weiter kann Profiling auch dazu dienen, personalisiertes und zielgerichtetes Marketing zu ermöglichen (vgl. Kapitel 3.5).

«In Bezug auf Finanzdienstleister lässt sich festhalten, dass beim Profiling mit hohem Risiko eine Datenschutzfolgeabschätzung getroffen werden muss.»

Diese Möglichkeiten sind umso wertvoller, als sie unter dem revDSG noch zusätzlich unterstützt werden. So kann zum Beispiel Profiling, unter Vorbehalt zusätzlicher Vorgaben gemäss Bankkundengeheimnis, ohne Zusatzanforderungen konzernweit vorgenommen werden, da Konzerngesellschaften datenschutzrechtlich nicht als Dritte gelten (Art. 26 Abs. 3 u. Art. 31 Abs. 2 Bst b revDSG).

Mit dem revDSG wird als Variante zum Profiling zudem das «Profiling mit hohem Risiko» eingeführt. Ein solches hohes Risiko liegt dann vor, wenn das Profiling «ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt» (Art. 5 lit. g revDSG). Diese Formulierung wiederholt im Wesentlichen zahlreiche Aspekte, welche letztlich auf jedes Profiling zutreffen, und liefert deshalb keine scharfe Abgrenzung zum «normalen» Profiling. Die Kriterien, die zu einem Profiling mit hohem Risiko gemäss Art. 5 lit g revDSG führen, müssen in der Praxis noch näher eingegrenzt werden.

In Bezug auf Finanzdienstleister lässt sich festhalten, dass beim Profiling mit hohem Risiko eine Datenschutzfolgeabschätzung getroffen werden muss (vgl. Art. 22 Abs. 1 u. 2 revDSG). Zusätzlich ist das Risiko einer solchen Datenbearbeitung durch gängige technische und organisatorische Massnahmen zu mindern (vgl. Kapitel 2.4).

2.3 Rechtfertigungsformen

In den meisten Fällen muss zur Datenbearbeitung durch eine Bank keine Zustimmung seitens des Kunden erfolgen. Nach dem Schweizer Datenschutzrecht ist die Bearbeitung von Personendaten grundsätzlich auch ohne Einwilligung der betroffenen Person oder einem anderen Rechtfertigungsgrund zulässig, sofern keine Persönlichkeitsverletzung vorliegt oder droht. Eine Persönlichkeitsverletzung

droht insbesondere dann, wenn eine Verarbeitung gegen die Datenschutzgrundsätze verstösst, etwa gegen die Gebote der Zweckbindung, Transparenz, Rechtmässigkeit oder Verhältnismässigkeit (z.B. mit der Ausprägung Datensparsamkeit). Rechtfertigungsgründe sind nach dem revDSG namentlich eine Einwilligung der betroffenen Person, ein überwiegendes privates oder öffentliches Interesse oder eine gesetzliche Pflicht zur Datenbearbeitung.

Die Praxisrelevanz der Frage der Rechtfertigung wird nachfolgend anhand von zwei Beispielen in Zusammenhang mit dem Grundsatz der Zweckbindung dargestellt. Dabei ist zwischen einer vertragsrechtlichen Einwilligung (nach Obligationenrecht, OR), einer strafrechtlichen (in Zusammenhang mit dem Bankkundengeheimnis) und einer datenschutzrechtlichen zu unterscheiden.

Werden Kundendaten zum Zweck der Erfüllung der vertraglichen Verpflichtungen der Bank erhoben, darf die Bank diese Daten nur dann ohne Einwilligung des Kunden für weitere Zwecke verwenden, wenn dies anderweitig gerechtfertigt ist. Die Verwendung dieser Daten zum Zweck der Bekämpfung der Geldwäscherei ist erlaubt, da es sich um eine gesetzliche Pflicht der Bank handelt. Die Nutzung von Personendaten zum Zweck der Einladung zu einem Kundenevent ist in der Regel durch ein überwiegendes privates Interesse der Bank gerechtfertigt und deshalb ohne Einwilligung möglich. Dieses Regelungskonzept steht im Gegensatz zum europäischen Datenschutzrecht. Nach dem Konzept der europäischen Datenschutzgrundverordnung (DSGVO) erfolgen sämtliche Bearbeitungen personenbezogener Daten grundsätzlich unrechtmässig, ausser ein gesetzlicher Erlaubnistatbestand rechtfertigt diese.

Grundsätzlich sind umso höhere Anforderungen an die Gültigkeit einer datenschutzrechtlichen Einwilligung zu stellen, je mehr Risiko eine Datenbearbeitung für eine betroffene Person birgt. In Fällen, in denen eine kundenseitige Einwilligung erforderlich ist, kann zwischen zwei Einwilligungsarten unterschieden werden:

- **Konkludente Einwilligung:** Eine Einwilligung kann in Anwendung etablierter rechtlicher Grundsätze wie z.B. von Treu und Glauben (Art. 6 Abs. 2 u. 3 revDSG) konkludent (d.h. durch schlüssiges Verhalten) erfolgen, wenn der Kunde angemessen aufgeklärt wurde und freiwillig handelt. Von einer solchen konkludenten Einwilligung ist zum Beispiel auszugehen, wenn der Kunde über neue Vertragsbedingungen informiert wird und diesen nicht innerhalb der angegebenen Frist widerspricht[8].
- **Ausdrückliche Einwilligung:** Eine ausdrückliche Einwilligung ist nur erforderlich, soweit sie vom Datenschutzgesetz vorgesehen ist. Auch die ausdrückliche Einwilligung folgt dem Regelungskonzept nach dem OR. Das bedeutet, dass der erklärte Wille unmittelbar aus den verwendeten Worten oder Zeichen hervorgehen muss (Art. 1 Abs. 2 OR). Die datenschutzrechtliche Anforderung an eine ausdrückliche Einwilligung entspricht jedoch nicht dem Formerfordernis der Schriftlichkeit gemäss OR. Nach revDSG ist entscheidend, dass die Einwilligung gestützt auf eine angemessene Information, bezüglich des Gegenstands der Einwilligung freiwillig, eindeutig und – aus Beweisgründen – dokumentierbar erfolgt. Demnach kann mit der richtigen Vertragsarchitektur und zielführender transparenter Information auch mit den «Allgemeinen Geschäftsbedingungen» (AGB) eine ausdrückliche Einwilligung erzielt werden oder aber im digitalen Kontext, zum Beispiel durch Anklicken eines entsprechenden Buttons.

8 Eine Einwilligung, die eine ausdrückliche Willenserklärung des Kunden erfordert, wird häufig auch als «Opt-in» bezeichnet. Gerade im datenschutzrechtlichen Kontext hat die Umschreibung «Opt-in» eine erhebliche Bedeutung.

Ob im konkreten Fall von einer ausdrücklichen oder einer konkludenten Einwilligung auszugehen ist, ergibt sich demgegenüber aus dem obligationenrechtlichen Verständnis (Art. 1 Abs. 2 OR).

Banken müssen darüber hinaus prüfen, ob gegebenenfalls über das Datenschutzrecht hinausgehende Einwilligungserfordernisse bestehen. Auf Personendaten von Bankkunden ist das Bankkundengeheimnis anwendbar. Bestimmte Bearbeitungsformen erfordern, dass der Kunde in die Aufhebung des Bankkundengeheimnisses einwilligt, damit Daten an Dritte weitergegeben werden dürfen, die nicht als Beauftragte der Bank qualifizieren. Weitere Einwilligungserfordernisse könnten sich aus den bestehenden Vereinbarungen mit den Bankkunden ergeben.

Unabhängig von der Frage nach der Rechtmässigkeit der Datenbearbeitung stellt sich die Frage nach möglichen Reputationsrisiken. Diese ergeben sich, sofern eine Diskrepanz zwischen derjenigen Datenbearbeitung besteht, welche die betroffene Person nach Treu und Glauben erwarten kann, und derjenigen, welche tatsächlich durchgeführt wird. Um eine solche Diskrepanz zu vermeiden, ist ein Risiko-Review-Prozess zu etablieren, worin Stakeholder aus verschiedenen Bereichen eine Strategie für den Umgang mit der Datenbearbeitung definieren. Darin sollte festgelegt werden, welche Datenbearbeitungen innerhalb des rechtlich zulässigen Rahmens geeignet sind, um die Reputation der Bank nach Massgabe ihrer Positionierung im Markt zu wahren bzw. auf welche Datenbearbeitung aus Reputationsgründen freiwillig verzichtet werden soll.

2.4 Technische und organisatorische Massnahmen (TOM)

Allgemeines
TOM sind Vorgaben, welche der Einhaltung der gesetzlichen Pflichten dienen. Die relevanten rechtlichen Vorgaben werden zunächst identifiziert und anschliessend durch die jeweiligen Experten in operationalisierbare Vorgaben, sogenannte Vorgaben für technische und/oder organisatorische Massnahmen (TOM-Vorgaben) übersetzt. Wenn Vorgaben für technische Massnahmen nicht oder nicht ausreichend greifen, sind kompensierende organisatorische Massnahmen in Form von TOM vorzusehen[9].

TOM-Vorgaben können daher den Besonderheiten der Aufbau- und Ablauforganisation der jeweiligen Bank hinreichend Rechnung tragen. Sie orientieren sich an Regeln der Berufskunde, am Stand der Technik, Branchenstandards oder Usanzen und sind damit dynamisch dem Wandel der Zeit unterworfen. Aus diesen Gründen müssen TOM-Vorgaben regelmässig auf ihre Eignung sowie Wirksamkeit überprüft werden. Dieses Vorgehen entspricht den Prinzipien von «Privacy by Design» und «Privacy by Default» (vgl. Art. 7 revDSG und Art. 25 DSGVO). Danach ist die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass insbesondere die Bearbeitungsgrundsätze wie zum Beispiel Zweckbindung, Transparenz, Rechtmässigkeit und Verhältnismässigkeit (z.B. mit der Ausprägung Datensparsamkeit) eingehalten werden. Diese ist bereits ab der Planung, d.h. in der Konzeptphase zu berücksichtigen.

9 In dieser Publikation wird nur auf ausgewählte TOM eingegangen. Eine umfassende Übersicht liefert der Eidgenössische Datenschutz und Öffentlichkeitsbeauftragte (EDÖB) im Leitfaden zu den technischen und organisatorischen Massnahmen zum Datenschutz.

Beispiele für TOM-Vorgaben[10]:

- Für **Vertraulichkeit, Integrität** sowie **Verfügbarkeit** kann auf die FINMA-Vorgaben zu Operationellen Risiken sowie CID (FINMA-RS 08/21 «Operationelle Risiken – Banken», insbesondere Anhang 3) und allgemeine ISO-Standards verwiesen werden.
- Für Aspekte wie **Richtigkeit, Zweckbindung, Datensparsamkeit** oder Grad der **Transparenz** werden sinnvollerweise Einsatzkonzepte verfasst, worin applikationsspezifische Vorgaben sowie **Kontrollen** für den Umgang mit Daten definiert werden.
- Ebenfalls denkbar sind Vorgaben für Graphical User Interfaces (GUI), um bspw. die **Datenbearbeitung** (Zweckbindung, Datensparsamkeit) innerhalb von Freitextfeldern zu regeln.
- Dasselbe gilt für Vorgaben der IT-Architektur, generell zum Beispiel für **Verfügbarkeit, Belastbarkeit, Kapazität** und **Wirksamkeitsnachweis** von IT-Systemen und spezifisch für **technische Schnittstellen**, welche einen Datenaustausch innerhalb der Bank oder mit Externen hinsichtlich Datenkategorie, Zweckbindung, Richtigkeit, Datensparsamkeit etc. definieren.
- Typische organisatorische Massnahmen, welche namentlich mangels Verfügbarkeit geeigneter technischer Massnahmen zwecks Risikomitigierung zum Einsatz kommen können, sind etwa streng funktionale **Zuteilung von Datenzugriffsrechten, Vieraugenprinzip, Beschränkung des Zugangs zu bestimmten Daten** oder **die vorgängige Bewilligungspflicht** zur Bearbeitung bestimmter Daten.

Beispiele konkreter technischer / organisatorischer Massnahmen

Der Schutz von Personendaten wird durch angemessene TOM-Vorgaben der (IT-) Sicherheit für die Wahrung der Vertraulichkeit, Integrität sowie Verfügbarkeit sichergestellt. Davon ist die Einhaltung bankkundengeheimnis- oder datenschutzrechtlicher Vorgaben durch allenfalls ähnliche TOM-Vorgaben anderer Fachbereiche des Businesses (1st Line of Defense) zu unterscheiden. Zum Beispiel dienen TOM-Vorgaben zur Anonymisierung oder Pseudonymisierung der (teilweisen) Aufhebung des Personenbezugs. Ohne Personenbezug sind datenschutzrechtliche bzw. bankkundengeheimnisrechtliche Vorgaben nicht mehr anwendbar.

Folgende technischen Möglichkeiten stehen nach heutigem Stand im Vordergrund:

- **Anonymisierung:** Bei der Anonymisierung von Daten werden personenbezogene Attribute (zum Beispiel Name und andere Identifikationsmerkmale einer Person) unwiederbringlich und irreversibel verändert. In der Folge kann nicht mehr auf die betroffene Person Rückschluss gezogen werden. Aus datenschutzrechtlicher Sicht bedeutet «Anonymisierung», dass die Betroffenen weder identifiziert noch identifizierbar sind. Sind Daten korrekt und vollständig anonymisiert (d.h. die Betroffenen sind weder identifiziert noch identifizierbar), liegen unstrittig keine Personendaten vor (vgl. Kapitel 2.1).
- **Pseudonymisierung:** Bei der Pseudonymisierung werden einzelne Merkmale in einem Datensatz nicht gelöscht, sondern verschleiert oder durch Pseudonyme, Kennzeichen oder einen Code ersetzt. Dies

10 Weitere Beispiele für TOM-Vorgaben finden sich in Guidelines verschiedener IT-Dienstleister oder Aufsichtsbehörden. Diese sind jedoch mit Vorsicht zu geniessen, da sie sich häufig lediglich auf die DSGVO bzw. EU-Recht beziehen und wesentliche Unterschiede hinsichtlich des übergeordneten allgemeinen Rechtsrahmens sowie branchenspezifischer Vorgaben der schweizerischen Rechtsordnung nicht berücksichtigen. Mit diesem Vorbehalt können solche Guidelines als Inspirationsquelle dienlich sein. Gute Beispiele dafür sind: «Datenschutz Sachsen-Anhalt Checkliste TOMs nach DSGVO» und «Das Standard-Datenschutzmodell (SDM) – ULD».

mit dem Zweck, die Bestimmung einer Person auszuschliessen. Pseudonymisierte Daten können somit nicht unmittelbar einer Person zugeordnet werden, sondern nur über eine Zuordnungsregel bzw. einen Schlüssel. Aus Sicht des Datenempfängers, liegt dann keine Bearbeitung von Personendaten vor, wenn dieser nicht über diesen Schlüssel verfügt. Pseudonymisierte Daten sind demzufolge nur aus Sicht des Datenempfängers anonymisiert. Demgegenüber kann der Datenverantwortliche die Daten gestützt auf den in seinem Besitz befindlichen Schlüssel wieder den betroffenen Personen zuordnen.

- **Verschlüsselung:** Bei der Verschlüsselung werden personenbezogene Daten durch einen Schlüssel in einen «Geheimtext» umgewandelt. Die Ausgangsinformationen werden dadurch nur noch unter Verwendung des passenden Schlüssels wieder lesbar. Der Zugriff auf diesen Verschlüsselungsschlüssel sollte unter der Kontrolle der Bank stehen und vor unberechtigten Zugriffen geschützt sein. Das Verschlüsselungsverfahren wie auch die Stärke des Verschlüsselungsschlüssels müssen den aktuellen Sicherheitsstandards entsprechen, sodass die Verschlüsselung als kryptographisch sicher betrachtet werden kann. Eine Übermittlung von CID sollte deshalb immer mit geeigneten technischen und organisatorischen Massnahmen besonders gesichert werden, zum Beispiel mit Verschlüsselung. Nach alledem ist Verschlüsselung kein eigenständiges Konzept, sondern ein technischer Anwendungsfall von Pseudonymisierung.

2.5 KI – Governance

Ein weiteres Thema, welches beim Umgang mit Daten in Zukunft immer mehr Banken beschäftigen wird, ist die Künstliche Intelligenz («KI»). Der Begriff wurde erstmals im Jahr 1956 während einer Konferenz am Dartmouth College verwendet[11]. Die Steigerung der Rechenleistung in den vergangenen 15 Jahren und die relativ einfache Verfügbarkeit von vielen Trainingsdaten für die Anwendung selbstlernender Algorithmen waren wesentliche Faktoren für den aktuellen KI-Boom. Verschiedene Methoden der KI werden häufig in weitere Teilbereiche aufgeteilt[12]:

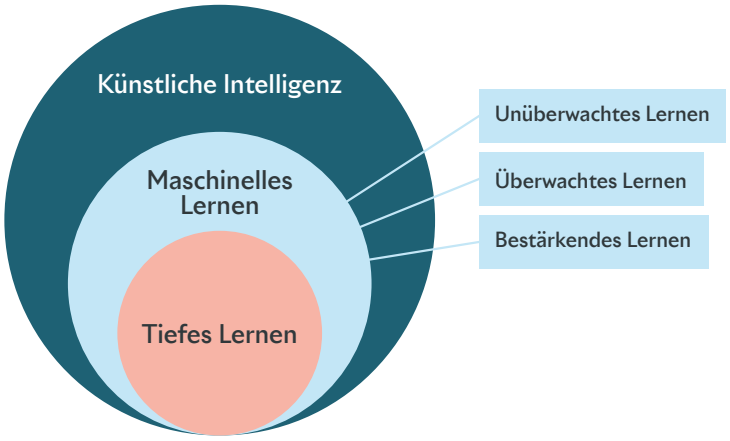
- **Künstliche Intelligenz:** KI beschreibt ein interdisziplinäres Forschungsfeld, welches das Ziel verfolgt, Maschinen (Computer) intelligentes Verhalten beizubringen.
- **Maschinelles Lernen:** «Machine Learning» ist eine Untergruppe der KI und beschreibt die Verwendung von Algorithmen, um Muster in Daten zu finden. Dazu gehören Methoden wie überwachtes Lernen («Supervised Learning»), unüberwachtes Lernen («Unsupervised Learning») und bestärkendes Lernen («Reinforcement Learning»).
- **Deep Learning:** DL ist eine Untergruppe von maschinellem Lernen, welche es Computern ermöglicht, noch komplexere Muster (z.B. in unstrukturierten Daten wie Audios, Videos, Bildern oder Texten) zu erkennen. Die Tatsache, dass diese künstlichen neuronalen Netzwerke mehrere Schichten enthalten, hat zum Namen «tiefes» Lernen geführt.

11 Vgl. P. McCorduck (1979), «Machines Who Think».

12 Vgl. T. Appenzeller (2017), «The AI revolution in science».

Abbildung 3

Die Teilbereiche von Künstlicher Intelligenz



Quelle: SBVg. In Anlehnung an EU AI-HLEG

Im Zusammenhang mit KI sind insbesondere folgende Aspekte wichtig:

- die **Qualität und die Differenziertheit der verwendeten Datensätze**, da undifferenzierte oder falsche Daten zu diskriminierenden oder falschen Ergebnissen führen können;
- auf KI basierende **Prozesse sollten erklärbar, d.h. transparent und nachvollziehbar sein**;
- die **Mitarbeitenden sollten entsprechend ausgebildet sein**, damit sie kontrollieren können, ob sich die automatischen Schlussfolgerungen innerhalb der vorgängig definierten Parameter bewegen und sie gegebenenfalls regulierend in die Prozesse eingreifen können.

Zu prüfen ist ebenfalls, ob neben der generellen datenschutzrechtlichen Informationspflicht (Art. 19 f. revDSG) ein aus dem Kundenvertrauen und dem Transparenzgrundsatz resultierendes zusätzliches Informationserfordernis hinsichtlich der Art der Datenbearbeitung durch KI-Anwendungen besteht. Ein allenfalls bestehendes Reputationsrisiko könnte durch entsprechende informative Massnahmen aufgefangen werden.

Entscheidungen über die aufgrund des Einsatzes von KI gewonnenen Ergebnisse werden aus Gründen der Kontrolle in den meisten Fällen den Mitarbeitenden der Banken vorbehalten sein. Sollten Entscheidungen ausschliesslich durch KI-Systeme ohne Intervention eines Mitarbeitenden getroffen werden, sind die möglichen Rechtsfolgen hinsichtlich der sogenannten automatisierten Einzelentscheidung zu prüfen und gegebenenfalls zu beachten (Art. 21 revDSG). Sofern Dienstleister der Banken im Rahmen der Nutzung von KI-Systemen Zugang zu Personendaten erhalten und/oder diese anderweitig bearbeiten, sind die datenschutzrechtlichen Vorschriften hinsichtlich der Auftragsdatenbearbeitung (z.B. Art. 9 revDSG) und gegebenenfalls auch hinsichtlich der Bekanntgabe von Personendaten ins Ausland (Art. 16 f. revDSG) zu prüfen.

«Entscheidungen über die aufgrund des Einsatzes von KI gewonnenen Ergebnisse werden aus Gründen der Kontrolle in den meisten Fällen den Mitarbeitenden der Banken vorbehalten sein.»

Zu beachten ist in diesem Zusammenhang, dass sich ein Auftragsbearbeiter datenschutzrechtlich nicht als echter Dritter im Sinne von Art. 31 Abs. 2 lit. c. revDSG qualifiziert und deshalb auch dann keine datenschutzrechtliche Einwilligung durch den Kunden erforderlich ist, wenn der Auftragsbearbeiter Zugang zu besonders schützenswerten Personendaten erhält. Zudem ist die Pflicht zur Information der betroffenen Personen eingeschränkt (vgl. Art. 20 Abs. 3 lit. c Ziff. 2 revDSG).

Sollten Dienstleister Kundendaten bearbeiten, sind auch die rechtlichen Voraussetzungen gemäss Bankkundengeheimnis (Art. 47 BankG) für den Beizug von Beauftragten zu berücksichtigen. Weiterhin ist die Anwendbarkeit des FINMA-RS 18/3 «Outsourcing – Banken und Versicherer» zu prüfen[13]. Der SBVg Cloud Leitfaden kann zur Beurteilung der in diesem Abschnitt genannten Vorgaben ebenfalls hinzugezogen werden, da dieser die rechtlich relevanten Aspekte bei der Weitergabe von Daten an Dritte (z.B. an Cloudanbieter) im Detail erläutert.

Verantwortungsvolle KI («Responsible AI»)

Der Einsatz von neuen Technologien wie KI kann neue Risiken mit sich bringen. Beispiele für mögliche Risiken sind u.a. Voreingenommenheit (Bias), ethische Herausforderungen, unkontrollierbare / nicht erklärbare Ergebnisse (Black Box), fehlende Robustheit gegenüber neuen Daten oder feindliche Angriffe. Es gilt daher eine Balance zwischen Innovation und Risikobereitschaft für den Einsatz dieser Technologien zu finden. Zur Identifikation, Beurteilung, Vermeidung und Kontrolle solcher Risken empfiehlt sich ein risikobasierter Ansatz. Entsprechende KI-Risiko-Rahmenwerke verfolgen typischerweise folgende vier Bereiche:

1. **Governance** (z.B. IT-Governance, Model Governance, rechtliche Beurteilung & Compliance, Rollen und Verantwortlichkeit, Ethik Boards)
2. **Data Management** (z.B. Datenschutz, Zugriffsrechte, Datenqualität, Datenkontrolle)
3. **AI Principles, Guidelines und Code of Conduct** (z.B. Erklärbarkeit, Fairness und Gleichberechtigung, Transparenz, Ethik, Sicherheit, Kontrolle, Robustheit und Rechenschaftspflicht)
4. **Kommunikation, Schulungen und Awareness-Building** (z.B. Peer-Review, Trainings für Mitarbeitende, Beobachtung der Aussensicht durch Ethik Trendradars)

Der verantwortungsvolle Einsatz von KI ist ein interdisziplinäres Forschungsfeld und enthält u.a. Forschungsfragen in technischen, ökonomischen, rechtlichen, sozialwissenschaftlichen und philosophischen Disziplinen. In den letzten Jahren wurden in all diesen Bereichen grosse Fortschritte gemacht (z.B. im Bereich der Erklärbarkeit von Algorithmen, AI Fairness, Verschlüsselung und Kryptographie). Auch in den nächsten Jahren sind hier grosse Fortschritte zu erwarten. Parallel dazu haben viele Staaten, internationale Standards setzende Organisationen, Unternehmen und Branchenverbände eigene Leitlinien (Principles und Guidelines) für den Einsatz von KI entwickelt. Aktuell laufen vermehrt Initiativen, die solche Leitlinien konkretisieren und operativ anwendbar machen sollen. Da dies ein sich rasant entwickelndes Feld ist, empfiehlt die SBVg den verantwortlichen Mitarbeitenden in Banken, sich in diesem Bereich laufend zu informieren und die aktuelle Forschung zu beobachten.

13 Wenn ein Dienstleister im Rahmen der Machine Learning Systeme Zugang zu einer bedeutenden Menge an Kundendaten erhält, die als Massen-CID qualifiziert (FINMA-RS 08/21 «Operationelle Risiken – Banken», Anhang 3, Rz. 53), und die Bank die jeweilige Dienstleistung darüber hinaus als wesentlich bewertet.

3 Anwendungsfälle

3.1 Nutzung von künstlicher Intelligenz für Compliance-Zwecke

Hintergrund

Banken analysieren kontinuierlich eine grosse Bandbreite von Kundendaten zum Zweck der Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung. Basierend auf den gesetzlichen Sorgfaltspflichten werden Personendaten wie Name, Geburtsdatum, Kontaktinformationen, Kopien der Identitätsnachweise und gegebenenfalls Informationen bezüglich der Vermögenssituation sowie Transaktionsdaten von den Banken erhoben, dokumentiert und bearbeitet. Die Hauptquelle solcher Kundendaten bleibt der Kunde selbst. Allerdings werden unterstützend auch Daten aus verschiedenen Drittquellen wie Datenbanken spezialisierter Anbieter und dem Internet beschafft.

«Eine effektive Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung ist für die Integrität des Schweizer Finanzplatzes elementar»

Im Rahmen der Datenverarbeitung zum Zweck der Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung können die Banken auf Lösungen zurückgreifen, die auf künstlicher Intelligenz, insbesondere auf Machine Learning, basieren (vgl. Kapitel 2.5). Der Vorteil des Machine Learning liegt in der Lernfähigkeit des Systems. Dank dieser können die Systeme neue Risikobereiche und Muster der Geldwäscherei und Terrorismusfinanzierung selbständig erkennen. Zudem steigt die Geschwindigkeit der Analysen und verschiedene Datenquellen können vollständig und einheitlich analysiert werden. Der Einsatz dieser Technologie dient in der Regel nicht als Ersatz für menschliche Entscheidungen, sondern dazu, die gesetzlich geforderten Prozesse nachhaltiger und effizienter zu gestalten. Entscheidungsträger bleibt der zuständige Mitarbeitende der Bank.

Eine effektive Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung ist für die Integrität des Schweizer Finanzplatzes elementar. Der entsprechend gute Ruf ist auch bei der internationalen Positionierung der Schweiz – zum Beispiel im «Arbeitskreis zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung» der Financial Action Task Force (FATF) – wichtig. Die FATF legt die internationalen Grundsätze fest und dient damit vor allem dem Schutz der Bankkunden. Denn nur auf Basis dieser international vereinbarten Grundsätze kann eine reibungslose Abwicklung internationaler Transaktionen gewährleistet werden.

Anwendungsmöglichkeiten

Auf Machine Learning basierende Anwendungen können in verschiedenen Stadien des Kundenlebenszyklus zum Einsatz kommen:

- **KYC und Onboarding:** Künstliche Intelligenz kann bei KYC-Prozessen und dem Onboarding helfen, die relevanten Daten automatisch zu identifizieren und den entsprechenden Risikoreport zu erstellen. Die auf künstlicher Intelligenz basierenden Systeme erkennen Personen, Orte, Fakten und Vorkommnisse und stellen sie nach selbsterlernten, dynamischen Mustern zusammen. Ausserdem filtern und bündeln sie doppelte oder ähnliche Informationen und kennzeichnen potenzielle Risiken. Die effiziente Vorbereitung der entscheidungsrelevanten Informationen ermöglicht den bankinternen Spezialisten, sich auf die relevanten Quellen zu konzentrieren und entsprechend begründete Entscheidungen zu treffen.

- **Transaktionsüberwachung:** Traditionelle Systeme der Transaktionsüberwachung identifizieren Verdachtsmomente ausschliesslich regelbasiert, zum Beispiel anhand von Wert oder Häufigkeit von Transaktionen. Abhängig von dem gewählten Schwellenwert kann es deshalb zu einem erhöhten Aufkommen falschpositiver Meldungen kommen, durch welche die Anzahl der durch die Mitarbeitenden abzuklärenden Fälle unnötig erhöht wird. Im Gegenzug führen zu niedrige Schwellenwerte dazu, dass Risiken unter Umständen nicht erkannt werden. Machine-Learning-Systeme erkennen unübliche Veränderungen von Transaktionsvolumina selbständig, und verbinden sie in der Analyse mit weiteren Kriterien der Transaktionsüberwachung, wie zum Beispiel Herkunft aus Staaten mit erhöhtem Risiko, Geschwindigkeit der Vermögensverschiebungen, Sanktions-, PEP[14]- und Terrorismusscreening. Diese dynamisch operierende Vorgehensweise weist insbesondere zwei Vorteile auf: Die Analyse erfolgt differenzierter und flexibler als im Rahmen der traditionellen statischen Systeme und durch die Verminderung falschpositiver Meldungen wird ein in diesem Bereich kritischer Zeitgewinn erzielt.

Mögliche Fragestellungen

Die jeweilige Anwendbarkeit der in Kapitel 2.5 aufgeführten Überlegungen bezüglich der Nutzung von KI ist zu prüfen. Die Bank muss das mit dem Einsatz von Machine Learning verbundene Risiko einschätzen und sollte ein entsprechendes Einsatzkonzept erstellen. Insbesondere gilt es zu dokumentieren, welche technischen und/oder organisatorischen Massnahmen im konkreten Fall angemessen sind. Bei der Wahl der TOM ist insbesondere auf die Einhaltung der datenschutzrechtlichen Bearbeitungsgrundsätze wie Zweckbindung, Transparenz, Rechtmässigkeit und Verhältnismässigkeit (z.B. mit der Ausprägung Datensparsamkeit) zu achten (vgl. Kapitel 2.4). Ausserdem ist das mit der Daten- und / oder Bearbeitungsart verbundene Risiko, zum Beispiel im Fall von besonders schützenswerten Personendaten (bspw. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen) sowie bei Profiling und in erhöhtem Masse bei Profiling mit hohem Risiko zu berücksichtigen (vgl. Kapitel 2.1 u. 2.2).

Die Bank sollte auch Prozesse implementieren, welche sicherstellen, dass die beteiligten Mitarbeitenden die Richtigkeit der Funktionalität bzw. der Ergebnisse überwachen und auf Plausibilität überprüfen können (vgl. Kapitel 2.5).

Auf ausschliesslich automatisierte Einzelentscheide ist zudem die Regelung von Art. 21 revDSG anwendbar. Umso mehr ist es auch unter diesem Aspekt sinnvoll, Prozesse zu implementieren, bei welchen den Mitarbeitenden nicht nur Pflichten zur Überwachung der Systeme, sondern auch Entscheidungskompetenzen eingeräumt werden (vgl. Kapitel 2.5 u. 3.2).

3.2 Kreditprüfung

Hintergrund

Banken können anhand von verifizierten Daten Informationen gewinnen, die für die korrekte Einstufung einer Kreditanfrage von Kunden verwendet werden können. Durch die zusätzlich gewonnenen Informationen kann die Bank mögliche Risiken frühzeitig identifizieren und im Risikobeitrag entsprechend

14 PEP steht für «politisch exponierte Personen».

berechnen[15]. Dadurch können den Kunden nicht nur personalisierte Offerten erstellt werden, sondern auch die Risiken besser gesteuert, sowie entsprechende Rückstellungen zielführender geplant und eingesetzt werden. Die nachfolgenden Ausführungen sehen mit Blick auf die Regelung für vollständig automatisierte Einzelentscheidungen gemäss Art. 21 revDSG immer einen Menschen als Entscheidungsträger bei der Kreditgewährung vor, d.h. der Kreditprüfungsprozess ist nicht vollständig automatisiert (vgl. Kapitel 2.5 u. 3.1). In der Praxis ist dies ein strategischer Entscheid des jeweiligen Finanzinstituts.

Anwendungsmöglichkeiten

Daten werden zur Kreditprüfung sowohl bei Firmen[16], als auch bei Privatpersonen (Hypothekar-, Konsumkredit) erhoben. Die Anwendungsbeispiele unterscheiden sich jedoch bei der Erhebung der Daten. Bei Firmen sind viele Informationen öffentlich einsehbar bzw. beschaffbar. Bei Privatpersonen muss zwar nicht unter revDSG (Art. 31 Abs. 2 Bst c), hingegen möglicherweise wegen dem Bankkundengeheimnis zuerst eine Einwilligung für die erweiterte Datenbeschaffung bei Dritten eingeholt werden. Die rasante technologische Entwicklung ermöglicht mittlerweile einen sehr effizienten und weitgehend digitalisierten Kreditprüfungsprozess mittels Machine Learning oder Natural Language Processing (NLP)[17].

Abbildung 4

Mögliche Datenquellen (Aufzählung nicht abschliessend)

Quelle: SBVg

15 Auch basierend auf historischen Verhaltensdaten von Kunden.

16 Unter dem revDSG «out of Scope».

17 NLP ist ein Teil der künstlichen Intelligenz und beschreibt eine Technik, um natürliche Sprache für einen Computer verständlich zu machen. Ziel ist es, dass ein Computer grosse Mengen und Textdaten verarbeiten und analysieren kann. Typische Anwendungen sind zum Beispiel maschinelle Übersetzer oder Spracherkennung.

Mögliche Fragestellungen

In Bezug auf die zur Kreditprüfung verwendeten Daten gibt es verschiedene Aspekte, die berücksichtigt werden sollten. So sollte die Qualität der verwendeten Daten jederzeit abschliessend und einwandfrei sein. Die Daten sollten zudem aktuell sein, die Realität korrekt abbilden und deren Herkunft muss klar ersichtlich sein [18]. Damit nur qualitativ einwandfreie Daten (gilt nicht nur für Personendaten) verwendet werden, bietet es sich aus datenschutzrechtlicher Sicht an, bei Zweifeln an der Herkunft der Daten oder fehlenden Verifizierungsmöglichkeiten auf eine Verwendung dieser Daten im Kreditprüfungsprozess zu verzichten. Diese Fragestellungen stellen sich namentlich bei Social Media und Internet als Datenquellen in erhöhtem Mass. Insgesamt empfiehlt es sich, sowohl den Grad der Datenqualität als auch die Datenherkunft transparent, nachvollziehbar und klar zu kommunizieren. Zusätzlich ist auch eine präzise Beschreibung der verwendeten Datenquellen denkbar. Weiter kann sich ein Finanzinstitut die Frage stellen, wie optimal informiert wird, damit das Kundenvertrauen in den (teil)automatisierten Kreditprüfungsprozess und den vertrauensvollen Umgang mit Daten jederzeit sichergestellt ist. Zudem ist es essentiell, mit technischen und/oder organisatorischen Massnahmen sicherzustellen, dass die Abfrage von externen Quellen nicht zu einer Verletzung des Bankkundengeheimnisses führt und dass nur diejenigen Daten erhoben, ausgewertet und für den Kreditentscheid verwendet werden, die auch tatsächlich erforderlich sind (vgl. Kapitel 2.4).

Damit ein Finanzinstitut sowohl dem rechtlichen Rahmen als auch der nötigen Vertrauensbasis der Kunden (insbesondere Privatkunden) gerecht werden kann, kann es gegebenenfalls erforderlich sein, beim Kunden eine ausdrückliche Einwilligung spezifisch für die Datenerhebung von externen Quellen einzuholen. Zusätzlich können dabei die erhobenen und verwendeten Daten auch offengelegt werden, damit die Herleitung der Kreditentscheidung transparent und nachvollziehbar ist. Um die diversen in Kapitel 2 beschriebenen Risiken bestmöglich zu adressieren, sollten die meisten Daten bei negativem Kreditentscheid wieder gelöscht und nur bei einer erfolgreichen Kreditzusage als Grundlage für die Entscheidung abgelegt werden [19]. Der Kunde wird dadurch geschützt, dass bei einem erneuten Antrag neue Daten erhoben werden müssen, da der Prozess aktuelle Daten als Grundlage fordert und somit keine historischen bzw. möglicherweise überholten Daten verwendet werden sollten [20]. Im Firmenkundengeschäft werden die obigen Ansätze bereits angewendet, jedoch noch sehr stark auf manuellen Abläufen basierend. Entsprechend ist die Herausforderung im Firmenkundengeschäft vor allem in der sinnvollen Automatisierung des Prozesses und somit im Datenaustausch (zwischen Banken, etc.) und des Daten-Stagings [21] zu finden.

18 Entspricht den datenschutzrechtlichen Grundsätzen der Rechtmässigkeit, Richtigkeit, Aktualität und Transparenz.

19 Es ist zu berücksichtigen, dass die Bank gegebenenfalls ein überwiegendes privates Interesse an der teilweisen Speicherung der Daten haben könnte, zum Beispiel hinsichtlich der Kontaktdaten und der Gründe des Nichtzustandekommens des Kredits.

20 Anwendungsfall der datenschutzrechtlichen Grundsätze der Richtigkeit und Aktualität.

21 Zusammenführung, Bereinigung und Transformation von Daten.

3.3 Trendanalysen und Benchmarking

Hintergrund

Der technologische Wandel beschleunigt Veränderungen im Kundenverhalten. Marktgrenzen verschwimmen zunehmend. Kundenbedürfnisse und kundenseitige Verhaltensänderungen frühzeitig zu erkennen und zu verstehen, ist daher auch für Banken ein zentraler Erfolgsfaktor. Dabei können Trendanalysen und Benchmarkings wertvolle Hilfsmittel sein. Nur wer Trends frühzeitig erfasst und seine Position im Markt kennt, kann sein Produktportfolio optimal positionieren und seine Vertriebsstrategien danach ausrichten.

Anwendungsmöglichkeiten

Banken verfügen mit Markt-, Transaktions- und Zahlungsverkehrsdaten über einen grossen Datenschatz für Trendanalysen und Benchmarkings, welche sowohl für interne wie auch für externe Anwendungen genutzt werden können.

Abbildung 5

Zwei Beispiele aus dem Bankalltag

BEISPIEL: TRENDANALYSE (INTERN)

Produktionsentwicklung und strategische Vertriebssteuerung

Trendanalysen können bei Banken intern verwendet werden, um Veränderungen im Kunden-/Kaufverhalten frühzeitig zu erkennen (z.B. steigende oder sinkende Nachfrage für einzelne Produkte, Themen oder Vertriebskanäle, Eintritt von Substitutionsprodukten). Entsprechende Frühwarnsysteme ermöglichen eine strategische Ausrichtung der Vertriebsressourcen und die Erschliessung neuer Kundenpotenziale. Frühzeitig erkannte Trends und Kundenbedürfnisse können in die Produktionsentwicklung einfliessen und für Produktionsinnovationen genutzt werden (z.B. für die Entwicklung innovativer ESG Anlagelösungen).

BEISPIEL: BENCHMARKING (EXTERN)

Business-Insight-Tool im E-Banking

Banken verfügen über wertvolle Daten zum Schweizer Unternehmensmarkt. Diese Informationen können anonymisiert ausgewertet und zum Beispiel in Form eines Business-Insight-Tools den Kunden zur Verfügung gestellt werden. Darin erhalten sie aggregierte Daten und Benchmarking-Insights (wie z.B. einen KMU-Profitabilitäts-Vergleich) auf der Basis von Daten aus verschiedenen Datenquellen (u.a. Transaktionsdaten, Marktdaten oder öffentliche Quellen). Solche Referenz- oder Vergleichswerte können für Unternehmen sehr wertvoll sein und ihnen helfen, ihre Effektivität und Effizienz zu steigern.

Quelle: SBVg

Mögliche Fragestellungen

Es stellt sich die Frage, welche Personendaten mit Bezug auf welche Geschäftsfelder die Bank ohne Weiteres analysieren darf, d.h. was von der Datenschutzerklärung der jeweiligen Bank abgedeckt ist und wie die Bearbeitungsgrundsätze mittels technischer/organisatorischer Massnahmen eingehalten werden können (vgl. Kapitel 2.4).

Unter anderem Anonymisierung und Aggregierung von Personendaten bergen ein Restrisiko hinsichtlich einer unbeabsichtigten Re-Identifizierbarkeit individueller, personenbezogener Daten. Hier soll mittels angemessener TOM sichergestellt werden, dass personenbezogene Daten nicht zurückverfolgt werden können und die Identität der Kunden auf keinen Fall erschlossen werden kann (z.B. durch Kreuzanalysen, Stichproben oder durch eine Kombination mit anderen Daten wie zum Beispiel Kundendaten oder öffentlich verfügbaren Daten) [22].

Wie hoch das Aggregierungsniveau bzw. die Gruppengrösse sein muss, damit kein Personenbezug anzunehmen ist, ist im Einzelfall zu bestimmen. Entscheidende Kriterien dabei sind u.a. die Anzahl der verwendeten Merkmale/Attribute, Hierarchien und Drill-Downs sowie die Grösse und Zusammensetzung der Grundgesamtheit. Darüber hinaus sollten nur sichere und effektive Anonymisierungsmethoden (basierend auf aktuellen wissenschaftlichen Methoden [23]) zur Anwendung kommen und die Analysen nur durch ausgewiesene spezialisierte Personen durchgeführt werden.

Die verwendeten Daten können systematische Fehler (Bias) enthalten. Diese können zum Beispiel entstehen, wenn der Kundenstamm einer Bank nicht repräsentativ für die Schweizer Gesamtbevölkerung oder die Unternehmenslandschaft ist. Zusätzlich ist von der Existenz von Scheinkausalitäten auszugehen. Es kann zum Beispiel zwischen zwei Grössen ein statistisch gemessener Zusammenhang (Korrelation) bestehen, ohne dass aber ein ursächlicher (kausaler) Zusammenhang vorhanden ist. Aktuelle wissenschaftliche Erkenntnisse, wie zum Beispiel im Bereich von «Algorithmic Fairness», sollten im Umgang mit Daten berücksichtigt werden (vgl. Infobox «Verantwortungsvolle Künstliche Intelligenz», Kapitel 2.5).

Des Weiteren sollten Trendanalysen und Benchmarking von Anfang an so gestaltet werden, dass bei Bedarf nachvollziehbare Erläuterungen gegeben werden können und die Eignung der Analyseergebnisse für bestimmte Fragestellungen und Anwendungsgebiete von den Nutzern abgeschätzt werden kann. Hierbei empfiehlt sich eine kurze und transparente Information im Kontext der Anwendung über die Zusammensetzung der Datensätze und die verwendeten Methoden der Datenverarbeitung.

22 Vgl. hierzu beispielsweise die Guideline der EDPB vom 10. April 2014 (ehemals WP29).

23 Beispiele für Anonymisierungs-Techniken und Anonymitäts- resp. Sicherheitsmasse: k-Anonymity, l-Diversity, t-Closeness, Anatomy, Differential Privacy oder Einsatz von synthetischen Daten.

3.4 Biometrische Authentifizierung

Hintergrund

Biometrische Authentifizierungsverfahren wie Fingerprint oder Gesichtserkennung via Smartphone finden vor allem bei digital affinen Bankkunden immer grösseren Zuspruch. Fälschungssicherheit, Einzigartigkeit und insbesondere die Einfachheit aus Kundensicht sind dabei die wichtigsten Aspekte. Biometrische Authentifizierungsverfahren erlauben der Finanzbranche beschleunigte und vereinfachte Prozesse an der Kundenschnittstelle und bilden zudem eine wichtige Voraussetzung für neue digitale Geschäftsmodelle. Mit der technischen Entwicklung werden für Banken auch neue Verfahren wie zum Beispiel die Stimm- und Spracherkennung interessant. Im telefonischen Kundenkontakt kann mit Hilfe der automatischen Stimmerkennung sowohl die Effizienz als auch der Komfort für die Kunden, durch den Wegfall von Authentifizierungsfragen, signifikant gesteigert werden. Während der Schilderung des Anliegens wird die Stimme mit dem hinterlegten Profil verglichen. Bei einer Übereinstimmung kann direkt mit der Bearbeitung des Anliegens weitergefahren werden.

Biometrische Merkmale lassen sich in der Regel nicht verändern. Dadurch sind biometrische Daten personengebunden und können immer einer bestimmten Person zugeordnet werden [24].

Anwendungsmöglichkeiten

Die Anwendungsmöglichkeiten im Bankalltag sind vielfältig. Das zweckmässigste biometrische Authentifizierungsverfahren leitet sich aus der konkreten Interaktion ab.

Abbildung 6

Biometrische Authentifizierungsverfahren im Bankalltag

Quelle: SBVg

Der Kunde legt typischerweise einmal fest, welche Authentifizierungsmethode er zukünftig bei einem Login im Mobile-/E-Banking oder auch bei einer telefonischen Kontaktaufnahme anwenden möchte. Grundsätzlich kann festgestellt werden, dass die rein digitale Form der Authentifizierung durchaus gute Ergebnisse liefert [25].

24 Die Ausführungen in diesem Kapitel beschränken sich auf die folgenden Verfahren: Fingerprint (Fingerabdruck), Gesichtsgeometrie (Gesichtserkennung) und Voiceprint (Stimm- und Sprecherkennung).

25 Vgl. auch FINMA-RS 16/7 «Video- und Online-Identifizierung».

Mögliche Fragestellungen

Grundsätzlich gilt es zwischen Fingerabdruck, Gesichtserkennung und Stimm- und Spracherkennung zu unterscheiden. Bei den ersten beiden erfolgt oft keine Datenspeicherung durch die Bank. Diese findet nach heutigem Stand der Technik auf dem kundeneigenen Mobiltelefon statt, weshalb die Bank nicht in der Verantwortung der gesetzlichen Datenschutzbestimmungen steht. Bei der Identifizierung via Fingerprint oder Gesichtserkennung ist nach revDSG Transparenz erforderlich, zum Beispiel in Form einer Datenschutzerklärung, nicht aber eine Einwilligung. Anders ist dies bei der Stimmerkennung, da der Stimmabdruck und somit die biometrischen Daten bei der Bank (On-Premises) oder in der Verantwortung der Bank (Cloud [26]) gespeichert werden, weshalb die relevanten Vorschriften des revDSG hier für die Bank relevant sind.

Generell ist zu beachten, dass für die Speicherung von biometrischen Daten (Technologie / Serverstandort) die geltenden Datenschutzbestimmungen eingehalten werden müssen, wie zum Beispiel das Recht der betroffenen Person auf Einsicht oder Korrektur sowie gegebenenfalls das Recht, die biometrische Authentifizierung zu deaktivieren und die relevanten Daten zu löschen.

Nebst dem Zweck der Authentifizierung kann ein biometrisches Profil auch für die Bestimmung weiterer Merkmale wie Alter, Geschlecht bis hin zum aktuellen Gemütszustand genutzt werden. Der Verwendungszweck des biometrischen Profils zur Identifikation muss daher abschliessend definiert werden und kann ohne zusätzliche Zustimmung des Kunden grundsätzlich nicht für weitere Zwecke verwendet werden (Art. 6 Abs. 3 revDSG). Ausnahmen von dieser Regel (diese gelten insbesondere für den Zweck der Strafverfolgung) müssen vom Gesetz vorgesehen sein (z.B. Art 31 Abs. 1 revDSG, siehe auch Kapitel 2 oben).

«Über datenschutzrechtliche Anforderungen hinaus ist gerade hier beim Thema der Kundenidentifikation naturgemäss die Einhaltung der Vorgaben zum Bankkundengeheimnis entscheidend.»

Über datenschutzrechtliche Anforderungen hinaus ist gerade hier beim Thema der Kundenidentifikation naturgemäss die Einhaltung der Vorgaben zum Bankkundengeheimnis entscheidend. Deshalb hat die FINMA in ihrem FINMA-RS 08/21 «Operationelle Risiken – Banken», insbesondere Anhang 3, die Vorschriften zum Umgang mit Kundenidentifikationsdaten (CID) präzisiert. Wie eingangs erwähnt, konkretisiert es mit Anforderungen hinsichtlich der TOM die Pflicht der Banken, die Vertraulichkeit von Kundenidentifikationsdaten in einer digitalisierten Welt sicherzustellen.

Eine transparente und verständliche Kommunikation betreffend Einsatz von biometrischen Erkennungssystemen kann die Hemmschwelle zur Nutzung seitens der Kunden gegenüber diesem Verfahren senken und zusätzlich mögliche Reputationsrisiken mitigieren. Aus Kundensicht ist neben der Reputation auch die Convenience ein treibender Faktor für eine rechtlich nicht erforderliche Zustimmung zur biometrischen Authentifizierung.

26 Siehe Cloud-Leitfaden der SBVg.

3.5 Personalisierte Angebote und Beratung

Hintergrund

Banken möchten jedem Kunden, entsprechend dessen individuellen Bedürfnissen und auf bestmöglicher Datenbasis, umfassende Angebote unterbreiten. Falls vom Kunden gewünscht, soll dieser dazu auch zielgerichtet beraten werden. Dabei sollen die Produkt- und Dienstleistungsangebote aufgrund der erkannten Interessen und Werte (z.B. Nachhaltigkeit) des Kunden individualisiert und konkretisiert werden. Die Zusammenstellung dieses Angebotes erfolgt a priori kanalunabhängig. Namentlich geht es darum, wesentliche Veränderungen der Verhältnisse der Kunden frühzeitig und möglichst systematisch zu erkennen, zum Beispiel infolge Heirat, Scheidung, Geburt von Kindern, Erbschaft, Änderung der beruflichen Tätigkeit oder Pensionierung. Aus solchen wesentlichen Veränderungen resultieren typischerweise auch veränderte Bedürfnisse in Bezug auf Bankdienstleistungen. Aber Achtung: Bei solchen Abklärungen ist zu beachten, dass typischerweise auch Drittpersonen wie zum Beispiel der Ehegatte der Kundschaft betroffen sein können. Solche Drittpersonen geniessen für sich selbst ebenfalls Datenschutz. Überdies geniessen sie nur den Schutz des Bankkundengeheimnisses, wenn sie ebenfalls Kunde der Bank sind. Gegebenenfalls sind solche Drittpersonen soweit nötig zum Beispiel via Kundschaft transparent in den Prozess mit einzubeziehen.

«Die Qualität respektive die Zielgenauigkeit wird besser, je umfangreicher die verwendeten Datensätze sind.»

Die Datenerhebung kann vollständig automatisiert oder aber – im Prinzip – vollständig manuell erfolgen. Mit digitalen Lösungen wird die Bank dem Kunden gegenüber allerdings umfassender, effizienter und zielgenauer auftreten können. Digitale Lösungen stellen zudem, einmal implementiert, einen identischen Qualitätsstandard gegenüber allen Kunden (unabhängig von der Person) sicher. Die Qualität resp. die Zielgenauigkeit wird besser, je umfangreicher die verwendeten Datensätze sind. Eine automatisierte Datenerhebung und ein individualisiertes Angebot erlauben letztlich eine wirklich kundenzentrierte Beratung.

Anwendungsmöglichkeiten

Spezifische Angebote können zeitlich optimiert werden. Ein Hypothekarangebot wird beispielsweise kurz vor Auslaufen einer bestehenden Festhypothek unterbreitet und nicht dann, wenn sich die Bank entscheidet, eine flächendeckende Kampagne zu Hypotheken für alle Kunden, unabhängig von deren Bedürfnissen, auszurollen. Aufgrund von systematisch erhobenen Kundenpräferenzen kann mit personalisiertem Marketing eine gezielte Bewerbung des Kunden bei neuen Bankdienstleistungen oder -produkten vorgenommen werden, zum Beispiel bei der Lancierung eines neuen Anlageproduktes. Die Analyseergebnisse können auch in direkte Beratungsdienstleistungen, etwa in einen strukturierten Anlageberatungsvertrag, einfliessen. Man denke etwa an die Erkenntnis, dass der Kunde Direktanlagen statt Anlagefondslösungen vorzieht oder vornehmlich nachhaltig investieren will. Die strukturierte Kenntnis des Kunden, seiner Präferenzen, Wertvorstellungen und Lebenssituation ermöglicht die auf seine Bedürfnisse abgestützte optimale Betreuung. Neben dadurch entstehenden Querverkäufen kann die Bank, gestützt auf die Analyseergebnisse, zudem den Zahlungsverkehr des Kunden zu dessen Schutz auf Anomalien hin überwachen (vgl. Kapitel 3.1 u. 3.3). Die Analyseergebnisse können auch in anonymisierter Form, d.h. ohne Möglichkeit von Rückschlüssen auf konkrete Kunden, zu statistischen oder strategischen Zwecken verwendet werden (vgl. Kapitel 2.4).

Mögliche Fragestellungen

Es stellt sich insbesondere die Frage, welche Daten die Bank mit Bezug auf welche Geschäftsfelder ohne Weiteres analysieren darf und will, ohne hierfür eine vorgängige Einwilligung des Kunden einzuholen (Transparenz ist ausreichend). Dies hängt von der Qualität der betroffenen Daten bzw. von den Umständen der konkreten Konstellation ab (vgl. Kapitel 2).

Die Bank kann Zugang zu Kundendaten haben, deren Verfügbarkeit nicht aus der originären Banktätigkeit resultiert. Dies ist zum Beispiel bei der Steuerberatung durch eine Bank der Fall, weshalb viele Bankkunden aus Diskretionsgründen ihre Steuerberatung bewusst bei einer anderen Bank als ihrer Hausbank in Anspruch nehmen.

Hier stellt sich die Frage, ob und unter welchen Voraussetzungen diese Daten für personalisierte Angebote verwendet werden dürfen. Was aus Sicht der Bank Sinn ergibt und durchaus im Interesse des Kunden gemeint ist, kann vom Kunden gegenteilig wahrgenommen werden, denn vom Kunden nicht angefragte Angebote können von diesem als Belästigung empfunden werden oder er misstraut grundsätzlich der Datenbearbeitung durch die Bank.

Die Datenanalyse und das gestützt darauf vorgenommene personalisierte Marketing ist bei Vorliegen der Grundanforderungen (vgl. Kapitel 2.3) in Anwendung des Grundsatzes von Treu und Glauben[27] immer ohne Weiteres zulässig, wenn kumulativ folgende Voraussetzungen erfüllt sind:

- Die Analyse basiert auf Daten, welche der Kunde selbst der Bank zur Verfügung gestellt hat. Gleich zu behandeln sind Daten, welche mit Wissen des Kunden bei Dritten erhoben wurden.
- Die Daten wurden von der Bank in Zusammenhang mit ihrer typischen Banktätigkeit erhoben. Letztere ist abhängig vom konkreten Geschäftsmodell der Bank und erfasst zum Beispiel bei einer Universalbank namentlich die drei Geschäftsfelder Konto- und Zahlungsverkehr, Finanzierungsgeschäft und Anlagegeschäft.

Erhebt die Bank aber vom Kunden stattdessen Daten im Rahmen einer nicht typischen Banktätigkeit wie zum Beispiel Erbschafts- und Steuerberatung, muss die Bank prüfen, ob für die Nutzung solcher Daten zu anderen Zwecken innerhalb der typischen Banktätigkeit falls nötig Transparenz zu schaffen ist. Dies ergibt sich nicht nur in Anwendung des Grundsatzes von Treu und Glauben, sondern auch aus der datenschutzrechtlichen Pflicht zur Zweckbindung und der Verhältnismässigkeit der Datenbearbeitung (vgl. Art. 6 Abs. 2 und Abs. 3 revDSG). Erklärt der Kunde, dass er personalisierte Angebote generell oder auch bloss themenspezifisch nicht mehr wünscht, hat die Bank dies umzusetzen. Dies ist in einem digitalen System einfacher als rein manuell. Eine vollständig digitale Datenerhebung wird in diesem Zusammenhang möglicherweise als Profiling qualifizieren. Je nach Sensibilität der Daten als solches mit normalem Risiko oder als solches mit hohem Risiko (vgl. Kapitel 2.2). Datenbeschaffung bei Dritten benötigt im Rahmen der allgemeinen Voraussetzungen dann keiner spezifischen vorgängigen Einwilligung des Kunden, wenn die von der Bank über den Kunden erhobenen Daten nach Treu und Glauben vom Erfahrungs- bzw. Erwartungshorizont des betreffenden Kunden abgedeckt sind (vgl. Kapitel 2.3).

27 Art 5 Abs. 2 revDSG statuiert ausdrücklich die Wichtigkeit des Grundsatzes von Treu und Glauben im Datenschutzrecht.

Beim Auftritt von Bankmitarbeitenden in Social Media kommt noch ein zusätzlicher Aspekt dazu: Hier sind aus Sicht zum Beispiel eines Kundenberaters ergänzend zu den gesetzlichen Regeln auch die internen Regeln der betreffenden Bank zum Umgang mit Social Media massgebend. Diese bestimmen über den Zugang zu und Nutzung von Social Media und den darauf befindlichen Daten.

3.6 Loyalitätsprogramme

Hintergrund
Loyalitätsprogramme beeinflussen die Einstellungen und das Kaufverhalten von Kunden positiv und stärken ihre Bindung zur Bank. Durch Loyalitätsprogramme können sich Banken differenzieren.

Unter Loyalitätsprogrammen werden in diesem Leitfaden Kundenbindungsinstrumente von Banken verstanden, die individuelle Präferenzen berücksichtigen und hierfür auf personenbezogene Daten zurückgreifen, um diese Programme zu individualisieren. Dabei werden zum Beispiel Kundendaten (wie Zahlungen) analysiert und persönliche Präferenzen herausgearbeitet.

Nicht differenzierende «Belohnungen», zum Beispiel eine Gutschrift von CHF 20 bei jeder Kontoeröffnung, welche für alle Kunden in gleichem Ausmass gewährt werden, fallen in diesem Zusammenhang nicht unter Loyalitätsprogramme, weil sie keine Bearbeitung von Personendaten verlangen.

Anwendungsmöglichkeiten
Loyalitätsprogramme lassen sich grob wie folgt klassifizieren:

1. **Cash-Back:** Bankkunden verdienen sich Vergünstigungen auf das Sortiment von Marken, die ihren persönlichen Interessen in Abhängigkeit mit Finanztransaktionen bei ihrer Bank entsprechen, zum Beispiel bei Kreditkartentranskationen. Die Bank schreibt dem Kunden die Vergünstigung nach dem Einkauf auf dem Konto gut und kann somit aus dem Kaufverhalten Informationen über die persönliche Präferenz des Kunden gewinnen.
2. **Punktesystem mit individualisierter Werbung:** Kunden verdienen Punkte in Abhängigkeit von Finanztransaktionen bei ihrer Bank, zum Beispiel bei Kreditkartentransaktionen, wenn sie die Kreditkarte einsetzen. Mit diesen Punkten können sie aus einem Katalog Produkte auswählen, die meist nichts mit der Bank zu tun haben. Die Angebote stehen allen zur Verfügung, jedoch wird die Werbung personalisiert durch das Auswerten von Personendaten, zum Beispiel des Kaufverhaltens über Transaktionsdaten.
3. **Neugeschäft**: Loyalitätsprogramme ermöglichen es, bestehende Kunden auch zur Nutzung weiterer Dienstleistungen zu gewinnen. Ein Kunde kann zum Beispiel in Abhängigkeit von Kreditkartentransaktionen oder Handelsaktivität Punkte gewinnen und diese für tiefere Zinsen beim Abschluss einer Neuhypothek oder höheren Sparzinsen beim Eröffnen eines Sparkontos eintauschen.

Den ersten beiden Programmtypen ist gemeinsam, dass die Banken intern vorhandene Kundendaten nutzen, diese aber im Prinzip mit einer Weitergabe von Personendaten an Drittparteien verknüpft sein könnten.

Mögliche Fragestellungen

Standardisierte (d.h. nicht individualisierte) Kundenbindungsprogramme sind aus einer Datenschutzperspektive eher unproblematisch.

Für die oben dargestellten individualisierten Loyalitätsprogramme könnten hingegen *statische Daten* (z.B. Name, Vorname, Geschlecht, Adresse, Telefonnummern, Alter, Haushaltsgrösse, Beruf, Ausbildungsabschluss, Kartennummer, Zahlungsarten und -daten) und *Geodaten* (z.B. Wohngebiet, Entfernung zum nächsten Unternehmensstandort) erhoben und verwendet werden.

Werden nun solche Daten auch für personalisierte Bewerbung von Drittprodukten verwendet, gehört dies nicht mehr zur Abwicklung der allgemeinen Bankbeziehung und sprengt damit den Rahmen der Bearbeitungszwecke, für welche die Daten ursprünglich vom Kunden der Bank überlassen worden sind. In diesem Fall besteht u.a. eine Informationspflicht und die Kunden sollten darauf hingewiesen und umfassend informiert werden, bevor sie in einem Loyalitätsprogramm beitreten [28].

Die erneute Informationspflicht kann entfallen, wenn der Kunde bereits bei der Geschäftseröffnung informiert wurde, dass Daten zum Zweck der personalisierten Werbung von Drittprodukten Dritten zur Verfügung gestellt werden. Darüber hinaus hat die Bearbeitung der Daten rechtmässig, nach Treu und Glauben sowie verhältnismässig zu erfolgen (vgl. Kapitel 2.3). Die Datenbearbeitung darf nur zu einem bestimmten, erkennbaren Zweck, hier der Durchführung von Loyalitätsprogrammen, vorgenommen werden.

«Loyalitätsprogramme können sowohl dem Kunden als auch der Bank einen Mehrwert bieten.»

Loyalitätsprogramme können sowohl dem Kunden als auch der Bank einen Mehrwert bieten. Die von Banken erhobenen Daten enthalten wertvolle Informationen. Auch für externe Parteien. In der heutigen Zeit, wo Daten ausserhalb der Finanzbranche allenfalls kommerzialisiert werden wollen, liegt die Vermutung nahe, dass Loyalitätsprogramme aus Kundensicht skeptisch wahrgenommen werden können, weil eine Weitergabe von persönlichen Daten vermutet werden könnte.

Eine klare Kommunikation zur Weitergabe von Kundendaten an Drittparteien – gerade auch wenn dies nicht geschieht – könnte Abhilfe und Vertrauen schaffen. Dabei ist auch zu prüfen, ob unter datenschutzrechtlichen Aspekten oder zumindest unter dem Bankkundengeheimnis sogar eine vorgängige Einwilligung des Kunden notwendig ist. Ganz allgemein muss auch hier die Datenschutzgesetzgebung, das Bankkundengeheimnis (Art. 47 BankG) und zu dessen Präzisierung mit Bezug auf den Umgang mit elektronischen Daten, das FINMA-RS 08/21 «Operationelle Risiken – Banken», Anhang 3, beachtet werden.

28 Beispielsweise mit einem klaren Hinweis im Rahmen der Eröffnung der Geschäftsbeziehung auf die auf der Website einfach auffindbaren Informationen zum Loyalitätsprogramm.

Schweizerische
Bankiervereinigung
Aeschenplatz 7
CH-4002 Basel
office@sba.ch
www.swissbanking.ch