bankenverband

Nutzung von Daten im Spannungsfeld von Kundenmehrwert und Datenschutz

Mai 2018

Andreas Krautscheid, Hauptgeschäftsführer, Staatsminister a.D.

Gemeinsame Positionen von Banken und FinTechs

„Die Digitale Transformation ist – auch für die Finanzbranche – eine der zentralen Herausforderungen. Dem begegnet der Bankenverband u. a. mit einer Zusammenarbeit mit Startups aus dem Finanzbereich, den FinTechs. Institutionalisiert wurde die Zusammenarbeit im Projektausschuss Digital Banking, der das Querschnittsthema Digitalisierung noch weiter intensiv vorantreibt. Der Projektausschuss ist ein hochkarätiges Gremium auf Ebene der Chief Digital Officer der Banken und führenden Köpfen der deutschen FinTech-Szene. Vorliegendes Dokument ist das Ergebnis intensiver Zusammenarbeit zwischen Banken und FinTechs."

Ansprechpartner Bankenverband:
Wulf Hartmann | Geschäftsbereich Recht | wulf.hartmann@bdb.de
Stephan Mietke | Geschäftsbereich Retail Banking, Banktechnologie | stephan.mietke@bdb.de
Tobias Tenner | Digital Banking | tobias.tenner@bdb.de

Einleitung

Die Finanzdienstleistungsbranche durchläuft einen tiefgreifenden digitalen Wandel, von dem in besonderer Weise das Privatkundengeschäft betroffen ist. Inzwischen hat eine Fülle neuer Anbieter mit innovativen Dienstleistungen und einer Vielzahl neuer Geschäftsmodelle den Markt betreten. Darunter sind – wie früher – Unternehmen, die einzelne Produkte erstellen oder vertreiben, aber ebenso Plattformen und ganze Ökosysteme, die Kunden, Produktanbieter, Abwickler oder Mehrwertdienstleister miteinander verknüpfen.

Auch der Bankenverband stellt sich dem digitalen Wandel: Er unterstützt die Zusammenarbeit zwischen Banken und FinTechs und trägt maßgeblich dazu bei, dass gemeinsame Positionen gefunden werden können. Diesem Positionspapier liegt die von beiden Gruppen erkannte Notwendigkeit zugrunde, die durch die Digitalisierung in immer größerem Ausmaß anfallenden Daten im Sinne der Kunden zu nutzen, ohne die Bedeutung des Datenschutzes aus den Augen zu verlieren.

Banken und FinTechs möchten den digitalen Wandel aktiv mitgestalten. Das Vertrauen der Kunden in den Schutz ihrer Daten zu wahren und zugleich zeitgemäße und nutzerfreundliche Anwendungen anzubieten ist dabei ein wesentlicher Erfolgsfaktor. Aus diesem Grund sehen unsere beiden Mitgliedergruppen es als unerlässlich an, dass der einzelne Kunde in die Lage versetzt wird, Überblick und Kontrolle über seine Daten zu behalten und souverän mit diesen Daten umzugehen.

Ausgangssituation

Die Digitalisierung bringt nicht nur den Unternehmen, sondern gerade auch den Kunden viele Vorteile: Mithilfe datenbasierter Analysen können ihr Nutzerverhalten und damit auch ihre Wünsche und Vorstellungen besser „verstanden“ werden. Den Unternehmen ist es auf diese Weise möglich, maßgeschneiderte Produkte zum richtigen Zeitpunkt anzubieten und einen individuellen Mehrwert für jeden Kunden zu erzielen.

Dieses Potential kann allerdings nur dann erschlossen werden, wenn der Nutzer tatsächlich einen echten Mehrwert für sich erkennt und zugleich ein angemessenes Maß an Sicherheit und Vertrauenswürdigkeit spürt. Letzteres ist unabdingbar, zumal auch das Datenschutzrecht vorsieht, dass der Einzelne bewusst und souverän über die Verwendung seiner Daten bestimmen können soll, sei es dass er bei Abschluss des Vertrages aufklärende Informationen erhält oder dann, wenn er eine Einwilligung unterzeichnet. Gerade in Deutschland lässt die Bevölkerung hinsichtlich der Nutzung oder Weitergabe von Daten eine gewisse Vorsicht und Skepsis walten, sofern Zusammenhang und Nutzen für sie nicht erkennbar sind. Werden die Kunden gefragt, ob sie mit einer breiteren Verwendung ihrer Daten einverstanden sind, reagiert typischerweise ein Großteil der Befragten zurückhaltend.

Im praktischen Leben zeigt sich allerdings häufig ein anderes Bild: Dienste, die bekanntermaßen auf einer sehr umfassenden Nutzung von Kundendaten basieren, dem Kunden aber (dadurch) einen spürbaren Mehrwert bieten, werden von der Bevölkerung gut angenommen; dies trifft auf soziale Netzwerke oder Messenger-Dienste, aber auch auf viele andere Produkte der digitalen Welt zu. Insofern sehen wir es – gerade vor dem Hintergrund der aktuellen Datenmissbrauchsvorwürfe gegenüber einzelnen Akteuren – als notwendig an, dass der informierte, bewusste und souveräne Umgang des Einzelnen mit seinen Daten die Regel ist.

Mit der neuen europäischen Datenschutzgrundverordnung (DSGVO) werden nun die Rahmenbedingungen für die Nutzung von Kundendaten weiter vereinheitlicht.

Damit ein echtes Level Playing Field für alle Marktteilnehmer entstehen kann, ist darauf zu achten, dass die Vorgaben EU-weit einheitlich umgesetzt und ausgelegt werden.

Mit Blick auf die Inhalte der DSGVO sehen wir allerdings kritisch, dass die Verordnung eine weitere Formalisierung und Ausdehnung von Datenschutzinformationen für die Kunden nach sich ziehen könnte. Nicht zuletzt wegen der hohen Sanktionsrisiken haben wir die Sorge, dass Kundeninformationen weiter „verrechtlicht" werden, was einer kundenorientierten Transparenz zuwiderlaufen würde. Ferner ist kritisch zu fragen, ob der (enge) Zweckbindungsgrundsatz im Datenschutzrecht angesichts der heutigen Innovationsdynamik und des breiten Erkenntnispotenzials von Big Data wirklich zeitgemäß ist oder nicht eher dazu führt, dass – auch im internationalen Vergleich – Chancen für Kunden und Anbieter verschenkt werden. Datenschutz muss sich auch daran messen lassen, dass er neuen Geschäftsmodellen in einer globalen Datenwirtschaft keine zu großen Hindernisse in den Weg legt und infolgedessen keine Fluchtwege über „Offshore"-Lösungen befördert. Eine ausgewogene Balance zwischen gesamtwirtschaftlichem Interesse und individuellen Schutzbedürfnissen muss ständig neu gesucht und optimiert werden.

Position I – Mehrwert für den Kunden durch Datennutzung

Dem Kunden kann durch Nutzung seiner Daten signifikanter Mehrwert geboten werden, ohne den Schutz seiner Daten oder die Privatsphäre einzuschränken.

Die Digitalisierung ermöglicht neue Wertschöpfungsansätze, von denen die Kunden in Form von besseren – d.h. qualitativ hochwertigeren, schnelleren und günstigeren – Produkten und Dienstleistungen profitieren können. Signifikanter Mehrwert entsteht beispielsweise im Zusammenhang mit

- einer geeigneten Identifizierung von Kundenbedürfnissen,
- einer Individualisierung von Produkten und Dienstleistungen,
- einem individuellen Schutz des Kunden vor wirtschaftlichen Verlusten und
- einer genaueren Risikosteuerung für die Bank.

Die damit verbundenen Ideen und Ansätze erfordern im Sinne der Erhebung, Verknüpfung und Anreicherung sowie dem Teilen dieser Daten mit Dritten allerdings eine intensivere Nutzung der Daten als früher.

Wenn ein Finanzdienstleister die Daten eines Kunden erhebt, kann es beispielsweise wichtig und sinnvoll sein, über reine Finanztransaktionen hinaus Kaufverträge und andere Vertragsdaten, spezifische Interessen oder Aufenthaltsdaten zu berücksichtigen. Mithilfe dieser zusätzlichen Daten wäre es dann leichter möglich, Einsparpotentiale zu realisieren, bessere Finanzkonditionen zu erhalten oder Kontomissbrauch früher als bisher zu erkennen.

Ideal wäre es auch, wenn Finanzdienstleister hierbei eigene Finanzdaten mit den Daten Dritter verknüpfen können, anstatt sie in abgeschotteten Datensilos jeweils neu erheben zu müssen. Denn viele der erwähnten Beispieldaten sind ja bereits bei anderen Service-Anbietern – zum Teil außerhalb des Finanzbereichs – vorhanden.

Diese erweiterten, zusammengeführten und angereicherten Daten sind eine bessere Gewähr dafür, dass die tatsächlichen Interessen und Bedürfnisse der Verbraucher bedient werden. Laut einer repräsentativen Umfrage aus dem Januar 2018 meinen drei Viertel der Bürger, dass Verbraucher bei Kaufentscheidungen heutzutage oft überfordert seien[1]. Hier könnten stärker datenbasierte Entscheidungsgrundlagen oder Empfehlungen bessere Orientierung geben.

1 Repräsentative Umfrage der GfK im Auftrag des Bankenverbandes „Verbraucherschutz aus Bürgersicht“, Januar 2018

Beispiele

- **Proaktives Budget- und Liquiditätsmonitoring**
  Banken könnten durch die Analyse der Transaktionsdaten im Zahlungsverkehr automatisch jenen Kunden Hilfe anbieten, deren finanzielle Situation sich infolge einschneidender Lebensveränderungen (z.B. Änderung des familiären Umfelds oder Arbeitslosigkeit) verschlechtert hat oder zu verschlechtern droht. Beispielsweise wäre es möglich, dass der Kunde in einem solchen Fall proaktiv eine aktualisierte Budget- und Liquiditätsplanung erhält. Auf diese Weise würde der Kunde zum frühestmöglichen Zeitpunkt auf bestmöglicher Datengrundlage beraten. Dies entspräche auch den Zielen aktueller Regulierungsbestrebungen.

  Ein solcher Service scheitert heute häufig daran, dass ein automatisiertes personalisiertes Auslesen des Verwendungszweckes nur mit ausdrücklicher Zustimmung des Kunden erlaubt ist (vgl. Art. 94 Abs. 2 PSD2 und Art. 6 Abs. 1 a DSGVO) und Kunden aufgrund von geringer Transparenz und Unsicherheit über die Datennutzung eine aktive Einwilligung scheuen.

- **Digitale Konto-/Depoteröffnung ohne Prozessbrüche**
  Ist ein Nutzer bereit, ein Konto online zu eröffnen, kann er den entsprechenden Prozess in wenigen Minuten durchführen. Um im Fall eines Verbindungsabbruchs oder absichtlicher Unterbrechung beim Ausfüllen des Online-Formulars die bereits aktiven Eingaben beizubehalten, speichert die jeweilige Website vorübergehend die Kundendaten, beispielsweise für einen Zeitraum von sieben Tagen. Ruft der Nutzer in dieser Zeit die Kontoeröffnungsstrecke erneut auf, werden seine einmal eingegebenen Informationen automatisch hochgeladen und er kann mit der Dateneingabe ohne zusätzlichen Aufwand fortfahren. Es besteht die Gefahr, dass mit der aktuell diskutierten europäischen e-Privacy-Verordnung diese Convenience-Gesichtspunkte verloren gehen.

- **Datennutzung aus Kontoinformationsdiensten**
  Ermächtigt ein Kunde im Zuge der neuen PSD2-Regulierung seine Bank, weitere Konten bei anderen Banken (im Wege eines Kontoinformationsdienstes) auf ihrer Onlinebanking-Plattform zu aggregieren, können die dadurch vorhandenen zusätzlichen Daten von der Bank so eingesetzt werden, dass sie dem Kunden diverse Mehrwerte schaffen.

  Allerdings ist heute in vielen Fällen noch nicht absehbar, welche Services hieraus genau entstehen werden. Da der Kunde bewusst für dieses Angebot optieren muss, ist obendrein zu erwarten, dass künftig neue Einwilligungen erforderlich sein werden und der Kunde folglich mit ständig geänderten oder erweiterten AGBs und Datenschutzbestimmungen konfrontiert werden wird.

Bestehende Barrieren

- Datenschutzrechtliche Prinzipien der Datensparsamkeit und der Zweckbindung:
  Es dürfen nur die für die Zweckerreichung konkret erforderlichen Daten benutzt werden. Die modernen Services – auch durch PSD2 getriggert – zeichnen sich jedoch dadurch aus, den Nutzer umfassend zu bedienen, sodass der Zweckfokus zunehmend „ausfranst".

- Intransparenz bzw. Unkenntnis des Kunden über die Nutzung seiner Daten:
  Die Verantwortlichen sind dazu verpflichtet, ausführliche Informationen über die Datenverarbeitung an den Kunden bzw. Betroffenen zur Verfügung zu stellen. Allerdings werden die Kunden mit entsprechend ausführlichen Datenschutzerklärungen schnell informativ „überflutet". Die durch die europäische Datenschutzgrundverordnung beförderte Detaillierung sowie die der Vermeidung von Sanktionsrisiken geschuldete Verrechtlichung der Sprache mindern für den Kunden die Verständlichkeit und Übersichtlichkeit – der ursprüngliche Zweck wird konterkariert.

- Der eigentlich richtige Grundsatz „Privacy by default" führt in der Praxis dazu, dass Anbieter ihre Nutzer in der digitalen Welt nicht wiedererkennen und ihren Service nicht proaktiv personalisieren können. Aus der „analogen" Welt – z.B. Bankfilialen – ist jedoch bekannt, dass der Kunde sehr wohl erkannt und persönlich betreut werden möchte.

Forderungen

Gesetzgeber und Datenschutzaufsicht sind aufgefordert, unter Gewährleistung des Datenschutzes einen der Datennutzung förderlichen Rahmen zu schaffen:

1. Relativierung des Prinzips der Datensparsamkeit, u.a. durch prinzipielle Erlaubnis der Nutzung öffentlich verfügbarer Daten (mit und ohne Personenbezug).

2. Befreiung des Zweckbindungsgrundsatzes aus einem zu engen Korsett:

   - Eröffnung von Möglichkeiten für den Kunden, vielfältige Verarbeitungszwecke akzeptieren zu können, und dies womöglich mit „einem Schritt" in den Grundeinstellungen oder zu Anfang der Nutzung eines umfassenden Services (mit Nachsteuerungsmöglichkeiten je nach Bedarf).
   - Mittelfristige Entwicklung vom überholten, weil nicht operationalisierbaren Grundsatzes der Zweckbindung hin zu einer Bindung (und Freigabe des Nutzers) für bestimmte Anwendungsklassen, Anbieter, Regionen oder andere konkret benennbare und für den Nutzer verständliche Ausprägungen der Datennutzung.

3. Akzeptanz zweistufiger Informationsvermittlungskonzepte, d.h. kurze, prägnante Informationen zur Gewährung des Überblicks (Stufe 1) und auf Nachfrage weitere Detail-informationen (Stufe 2) – siehe dazu auch unten Ausführungen zu Position II.

Flankierende Maßnahme(n) durch Banken/FinTechs

- Förderung der Kundenakzeptanz durch stärkere Kommunikation der Vorteile einer erweiterten und aggregierten Nutzung von Daten für den Kunden. Offensichtliche Use Cases sind die bessere Beratung des Kunden auf breiterer Datengrundlage, die Verbesserung in die Zukunft gerichteter Finanzszenarien, die Verhinderung von Betrug und vieles mehr.

- Aufzeigen von Möglichkeiten zur Standardisierung, um das Kundenvertrauen zu stärken. Möglichkeiten sind entsprechende Leitlinien, ein Code of Conduct oder ein der digitalen Welt angepasstes „Bankgeheimnis 2.0“.

Position II – Adressatengerechte Transparenz bei der Datennutzung

Ein an den Kundenbedürfnissen ausgerichtetes Transparenzkonzept hinsichtlich Datennutzung ist der richtige Ansatz, um die Datensouveränität des Verbrauchers zu stärken und Vertrauen in die Datenfreigabe für innovative Produkte zu schaffen.

Jeder Rahmen zur Förderung der Datennutzung im Sinne des Kunden muss gewährleisten, dass die Souveränität des Nutzers über seine Daten und der Schutz der Privatsphäre gewahrt bleiben. Hierzu ist es erforderlich, praxisgerechte Transparenzkonzepte und Steuerungsinstrumente zu entwickeln und zu implementieren.

Derzeit steht aufgrund des Sanktionsrisikos aus der EU-Datenschutzgrundverordnung die rechtliche Absicherung der Anbieter im Vordergrund, weshalb als Datenschutzerklärung meist ein ausführliches Dokument dient, das im sperrigen Juristendeutsch abgefasst ist. Dieses Dokument bietet zwar höchstmögliche (rechtliche) Transparenz, die eigentlich avisierte Verständlichkeit für den Nutzer bleibt jedoch häufig auf der Strecke.

Notwendig ist somit ein Transparenzprinzip, das nicht nur der juristischen Genauigkeit Rechnung trägt, sondern dem Kunden dadurch entgegenkommt, dass folgende Kernfragen kurz und bündig und damit für den Rechtslaien verständlich beantwortet werden:

- Wer nutzt die Daten (Anbieter, Dritte)?
- Welche Daten werden genutzt (nach Kategorien von Daten)?
- Für welche Zwecke werden die Daten genutzt?
- Werden die Daten weiterveräußert?
- Wo werden die Daten gespeichert/verarbeitet?

Beispiele

- **Lebensmittelampel:** Die Lebensmittelampel macht es vor: Sie soll den Verbraucher schützen, wenn dieser aufgrund mangelnden Vorwissens oder fehlender Informationen die Inhaltsstoffe eines Lebensmittelproduktes nicht zuverlässig einschätzen kann. Mittels einfacher und verständlicher Darstellungen soll auf einen Blick vorab erkennbar sein, ob das Produkt bestimmte Grenzen von Nährstoffgehalten überschreitet und so zu einer ungesunden Ernährung beiträgt.

- Auch bei Datenschutzerklärungen ist es oftmals so, dass es dem Kunden ohne ein spezifisches, in diesem Fall juristisches Grundverständnis kaum möglich ist, einen Einblick in die Verarbeitung seiner personenbezogenen Daten zu nehmen. Auch an dieser Stelle könnte eine verständliche und einheitliche Symbolik Abhilfe schaffen. Auf der ersten Seite der Datenschutzerklärungen sollte dabei eine Übersicht der Symbole mitsamt einem Erläuterungssatz zu finden sein, der die Datennutzung der Dienstleistung aufzeigt, die der Nutzer in Anspruch nehmen möchte.

Bestehende Barrieren

- Mangelnde Praxistauglichkeit der stark formalisierten Informationspflichten des Datenschutzrechts sowohl in Bezug auf Länge als auch auf die verwendete Rechtssprache.

- Fehlende Transparenzstandards bei Datenschutzinformationen: Diese sind strukturell anbieterindividuell und erschweren damit einen anbieterübergreifenden Vergleich für den Kunden.

Forderungen

Wir fordern eine Reihe von Maßnahmen hinsichtlich der Vereinfachung von Datenschutzerklärungen bei gleichzeitig verbesserter Akzeptanz durch die Nutzer. Im Einzelnen:

4. Förderung und Akzeptanz eines modifizierten Transparenzkonzepts durch den Gesetzgeber bzw. die Datenschutzaufsicht, das aus zwei Stufen besteht:

   - Betonung des Aspekts der Verständlichkeit bei der Verbraucherinformation zur Datennutzung, zum Beispiel in Form von Symbolen oder Icons.
   - Detaillierte Information bzw. Erläuterung der Symbole oder Icons mit rechtsverbindlicher Wirkung auf Nachfrage bzw. an zentraler Stelle eines Dienstes oder einer Website.

5. Förderung eines konkreten, einheitlichen Standards zur vereinfachten Darstellung von Informationen und „Botschaften“ (z.B. Icons, Stichpunkte, One-Pager).

6. Konstruktive Begleitung/Unterstützung etwaiger ergänzender branchenspezifischer Standards durch die zuständigen Datenschutzbehörden.

Flankierende Maßnahme(n) durch Banken/FinTechs

- Entwicklung eines Transparenzkonzepts als Hilfestellung oder sogar Best Practice für Mitglieder/Banken. Anhand dieses Konzepts sollen dem Kunden einfach und leicht verständlich der Umfang und die Grenzen der Nutzung seiner Daten aufgezeigt werden, sodass er die Tragweite seiner Datenfreigabe (z.B. im Rahmen des Vertrages oder durch gesonderte Einwilligung) nachvollziehen kann. Gleichzeitig könnte das Konzept Standards für den Datenschutz und die Datensicherheit innerhalb des bestehenden Rechtsrahmens setzen und damit zu einer Harmonisierung bei der Anwendung und Auslegung der Datenschutzvorschriften beitragen.

- Erstellung eines sektorspezifischen Datenschutz-Glossars, das dem Nutzer auf verständliche Weise die datenschutzrechtlich am häufigsten auftretenden Begriffe im Zusammenhang mit Finanzdienstleistungen erläutert.

Position III – Einfache Steuerbarkeit der Datennutzung über ein Datenschutz-Cockpit

Der Kunde soll die Anbieternutzung seiner Daten einfacher und bequemer als bisher steuern sowie nachvollziehen können. Damit soll er befähigt werden, die Kontrolle über seine Daten bewusst und souverän auszuüben.

Voraussetzung hierfür ist, dass der Kunde hinreichende Transparenz über die beabsichtigte Datennutzung durch den Anbieter oder gegebenenfalls durch dritte Parteien hat (siehe unter anderem Ausführungen oben zur Position II).

Rechtsgrundlage der Datenverarbeitung

Der Kunde sollte grundsätzlich in der Lage sein, die Datennutzung – z.B. im Rahmen eines Vertragsverhältnisses oder auf Basis einer Einwilligung – mit einer Willenserklärung zu steuern. In bestimmten Fällen ist allerdings eine Datenverarbeitung schon aufgrund gesetzlicher Vorgaben (Stichworte: verantwortungsvolle Kreditvergabe, Betrugsprävention) oder aufgrund einer Interessenabwägung (Stichworte: Austausch mit Kreditauskunfteien, Nutzung von Daten zu Werbezwecken) legitim. Dann muss eine Unterrichtung ausreichen – im Falle der Interessenabwägung mit der Möglichkeit zum Opt-out. Eine gesonderte Kundenzustimmung zur Nutzung der Daten im Rahmen eines Vertragsverhältnisses ist überflüssig: Kann der Vertrag nicht ohne Nutzung/Verarbeitung der Daten erfüllt werden, wäre eine Einwilligungslösung irreführend.

Im Falle einer vertraglichen Erklärung mit Datenverarbeitungsrelevanz oder einer gesonder-ten Einwilligung in die Datenverarbeitung sollte diese für den Betroffenen durch eine einfache Bestätigung, z.B. per Klick, möglich sein. Gerade bei Online-Prozessen führen Auswahlmöglichkeiten wie „Check-Boxen“ mit einer Vielzahl von Optionen nachweislich zu hohen Abbruchraten, da sie für den Kunden nicht nur zeitraubend sind, sondern zum Teil Entscheidungen verlangen, die den Kunden in der jeweiligen Situation leicht überfordern können. Anstelle von „Check-Boxen“ kann eine prägnante Information zur Datennutzung (siehe Position II) und gegebenenfalls ein Link auf ergänzende Bedingungen und Erklärungen sinnvoll sein, um den Kunden besser darüber zu informieren, unter welchen Bedingungen er der Datennutzung zustimmt.

Steuerbarkeit durch Datenschutz-Cockpit

Das datenschutzrechtliche Leitbild sieht vor, dass der Betroffene (im Rahmen der Einwilligung oder Vertragsvereinbarung) grundsätzlich selber entscheiden können soll, wer seine Daten wofür und in welchem Umfang verarbeiten darf. Das schließt auch seine Rechte auf Auskunft, auf Berichtigung oder Löschung, auf Einschränkung der Verarbeitung oder ein Widerspruchsrecht gegen die Verarbeitung sowie das Recht auf Datenübertragbarkeit mit ein. In der Praxis allerdings ist es für den Einzelnen aufgrund der Vielzahl seiner Vertragspartner und der unterschiedlichen Vertragsverhältnisse kaum möglich, die Übersicht zu behalten und effektiv die Kontrolle über seine Daten auszuüben.

Bessere Ergebnisse würde ein nutzerfreundliches digitales Datenschutz-Cockpit versprechen, mit dem auf einen Blick erkannt und – soweit möglich – gesteuert werden kann, welche Daten von welchen Anbietern zu welchem Zweck und in welchem Ausmaß genutzt werden. Über das Cockpit könnte der Nutzer zudem festlegen, welchen Online-Unternehmen er vollständige persönliche Daten anvertrauen und wem gegenüber er nur unter Pseudonym auftreten möchte. Einmal erteilte Zugriffsberechtigungen ließen sich auch nachträglich ändern oder widerrufen; dazu sollte es ein Protokoll über die Zugriffe geben. Das Cockpit sollte dem Kunden gegebenenfalls in standardisierter Form eine einfache und übersichtliche Darstellung anbieten.

Eine Cockpitlösung könnte einerseits von datenverarbeitenden Unternehmen innerhalb des Nutzerprofils bereitgestellt, andererseits aber auch von vertrauensvollen Drittanbietern (Trusted Parties) angeboten werden, die das Daten- und Identitätsmanagement – ähnlich den bankkontenaggregierenden Personal-Finance-Management-Diensten – an einer zentralen Stelle zusammenführen. Vergleichbar mit der „Social-Login"-Funktionalität, wie sie von Facebook, Google, LinkedIn, Xing oder Twitter bekannt sind, würde dieser Daten- und Identitätsmanagementdienst vor einem Zugriff auf die Kundendaten durch einen datennachfragenden Anbieter den Kunden darauf hinweisen, welche Daten für den Zugriff benötigt und daher übertragen werden. Der Nutzer würde hierdurch in eine Kontrollposition versetzt.

Erste Bemühungen von einzelnen US-amerikanischen Plattformanbietern zielen darauf ab, dem Nutzer die Möglichkeit zu geben, seine „Privatsphäre-Einstellungen" festzulegen. Diese Bestrebungen gehen uns allerdings nicht weit genug. Es wird dem Anwender zwar ermöglicht, die über sein Online-Nutzerverhalten protokollierten und gespeicherten Daten zu bearbeiten und zu löschen. Es fehlt jedoch der transparente und individuelle Gestaltungsfreiraum mit Blick auf die Datenfreigabe im Vorfeld der Nutzung.

Beispiele

- **Daten-/Identitätsmanagement-Plattform**
  Das Datenschutz-Cockpit könnte im Rahmen einer zentralen Daten-/Identitätsmanagement-Plattform zusammengeführt werden. Diese Plattform würde ihren Usern eine Art Internet-Generalschlüssel (single sign-on) für verschiedene Dienste bieten. Über ein sogenanntes „Permission Center" kann die Freigabe von Nutzerdaten kontrolliert und verwaltet werden: Nutzer können die Freigabeeinstellungen der Daten bei der Verknüpfung mit einem neuen Dienst individuell einstellen. Dabei entscheidet der Nutzer, welche Daten an wen übertragen und zu welchen Anlässen genutzt werden dürfen. Die Daten können jederzeit angepasst und wieder gelöscht werden. Der Nutzer kann ferner den gewünschten Grad an Bequemlichkeit einstellen, anhand dessen sich für die jeweiligen Dienste beispielsweise ergibt, ob Kontakt-, Bank- oder Versanddaten automatisch übertragen werden.

Bestehende Barrieren

- Unklarheit hinsichtlich der Auslegung des Datenschutzrechts und drohender Konsequenzen im Falle eines Verstoßes gerade bei anbieterübergreifenden Plattformlösungen. Die Nachweispflicht für die erforderliche Rechtsgrundlage bei der Verarbeitung personen-bezogener Daten liegt im Zweifels-/Streitfall beim Anbieter, was Anreize zur Einholung einer expliziten Kundeneinwilligung schafft, die wiederum die Kunden-Convenience schmälert.

- Hohe Komplexität und Aufwand bei der Konzeption und Umsetzung eines solchen Datenschutz-Cockpits.

Forderungen

7. Akzeptanz einer strukturierten Informations- und Steuerungsplattform insbesondere unter dem Blickwinkel Datenschutzrecht und Wettbewerbsrecht.

8. Für Fälle, in denen es der datenschutzrechtlichen Einwilligung bedarf:

   - Ermöglichung praxistauglicher Einwilligungslösungen, die für den Nutzer einfach nutzbar und leicht verständlich sind. Hierzu ist es notwendig, dass der Gesetzgeber solche Lösungen konkret beschreibt und in einen passenden Rechtsrahmen einbettet.
   - Ermöglichung einer einfachen – möglichst pauschalen – Kundenzustimmung ohne Erfordernis einer separaten, expliziten Zustimmung zu Einzelaspekten der Datennutzung
   - Der Freiwilligkeitsgrundsatz der Einwilligung (gemäß Art. 7 DSGVO) sollte erfüllt sein, wenn der Betroffene die Möglichkeit zum Opt-out bei einer über die Vertragserfüllung hinausgehenden Datennutzung hat.

Flankierende Maßnahme(n) durch Banken/FinTechs

- Identifizierung bereits existierender Standards für ein Datenschutz-Cockpit

- Bewertung einer möglichen Umsetzung durch die Finanzwirtschaft

Anhang: Übersicht der Forderungen

Position I – Mehrwert für den Kunden durch Datennutzung

1. Relativierung des Prinzips der Datensparsamkeit, u.a. durch prinzipielle Erlaubnis der Nutzung öffentlich verfügbarer Daten (mit und ohne Personenbezug).

2. Befreiung des Zweckbindungsgrundsatzes aus einem zu engen Korsett:
   - Eröffnung von Möglichkeiten für den Kunden, vielfältige Verarbeitungszwecke akzeptieren zu können, und dies womöglich mit „einem Schritt“ in den Grundeinstellungen oder zu Anfang der Nutzung eines umfassenden Services (mit Nachsteuerungsmöglichkeiten je nach Bedarf).
   - Mittelfristige Entwicklung vom überholten, weil nicht operationalisierbaren Grundsatzes der Zweckbindung hin zu einer Bindung (und Freigabe des Nutzers) für bestimmte Anwendungs-klassen, Anbieter, Regionen oder andere konkret benennbare und für den Nutzer verständliche Ausprägungen der Datennutzung.

3. Akzeptanz zweistufiger Informationsvermittlungskonzepte, d.h. kurze, prägnante Informationen zur Gewährung des Überblicks (Stufe 1) und auf Nachfrage weitere Detailinformationen (Stufe 2) – siehe dazu auch unten Ausführungen zu Position II.

Position II – Adressatengerechte Transparenz bei der Datennutzung

4. Förderung und Akzeptanz eines modifizierten Transparenzkonzepts durch den Gesetzgeber bzw. die Datenschutzaufsicht, das aus zwei Stufen besteht:
   - Betonung des Aspekts der Verständlichkeit bei der Verbraucherinformation zur Datennutzung, zum Beispiel in Form von Symbolen oder Icons.
   - Detaillierte Information bzw. Erläuterung der Symbole oder Icons mit rechtsverbindlicher Wirkung auf Nachfrage bzw. an zentraler Stelle eines Dienstes oder einer Website.

5. Förderung eines konkreten, einheitlichen Standards zur vereinfachten Darstellung von Informationen und „Botschaften“ (z.B. Icons, Stichpunkte, One-Pager).

6. Konstruktive Begleitung/Unterstützung etwaiger ergänzender branchenspezifischer Standards durch die zuständigen Datenschutzbehörden.

Position III – Einfache Steuerbarkeit der Datennutzung über ein Datenschutz -Cockpit

7. Akzeptanz einer strukturierten Informations- und Steuerungsplattform insbesondere unter dem Blickwinkel Datenschutzrecht und Wettbewerbsrecht.

8. Für Fälle, in denen es der datenschutzrechtlichen Einwilligung bedarf:
   - Ermöglichung praxistauglicher Einwilligungslösungen, die für den Nutzer einfach nutzbar und leicht verständlich sind. Hierzu ist es notwendig, dass der Gesetzgeber solche Lösungen konkret beschreibt und in einen passenden Rechtsrahmen einbettet;
   - Ermöglichung einer einfachen – möglichst pauschalen – Kundenzustimmung ohne Erfordernis einer separaten, expliziten Zustimmung zu Einzelaspekten der Datennutzung;
   - Der Freiwilligkeitsgrundsatz der Einwilligung (gemäß Art. 7 DSGVO) sollte erfüllt sein, wenn der Betroffene die Möglichkeit zum Opt-out bei einer über die Vertragserfüllung hinausgehenden Datennutzung hat.

Impressum | Herausgeber: Bundesverband deutscher Banken e. V., Postfach 040307, 10062 Berlin | Verantwortlich: Oliver Santen
bankenverband.de | Druck: PieReg Druckcenter Berlin GmbH | Foto: fotolia kras99 | Stand: Mai 2018

So erreichen Sie den Bankenverband

Per Post:
Bundesverband deutscher Banken
Postfach 040307
10062 Berlin

Per Telefon:
+49 30 1663-0

Per E-Mail:
bankenverband@bdb.de

Internet:
bankenverband.de