Datenverwendung: Von der **Zweckbindung** zum **Datenschutzcockpit**

Von Swantje Benkelberg

Quelle: pixabay

Die Datenschutz-Grundverordnung hat die über Verbraucher hereinbrechende Informationsflut in Sachen Datenschutz kräftig steigen lassen – und doch nicht für mehr Transparenz gesorgt. Der Bankenverband hat deshalb praktische Verbesserungen in Sachen Datenschutz und Datenverwendung angemahnt und wünscht sich zum Beispiel eine Lockerung der Zweckbindung. Das Zukunftskonzept eines „Datenschutzcockpit", über das der Verbraucher die Verwendung seiner persönlichen Daten zentral für alle seine Vertragspartner steuern kann, ist aufgrund einer Reihe offener Fragen wohl eher Zukunftsmusik. Red.

Die Analyse und Verwendung verfügbarer Daten wird im Zuge der Digitalisierung immer wichtiger – auch für Kreditinstitute. Doch im Zuge der Datenschutzdiskussionen gewinnt gleichzeitig der Mehrwert an Bedeutung, der für den Kunden durch die Nutzung seiner Daten entsteht. Nur dann wird er seine Einwilligung geben. Signifikanter Mehrwert kann durchaus auch geboten werden, ohne den Schutz persönlicher Daten oder der Privatsphäre einzuschränken. Trotzdem scheitert manches, was möglich wäre, an unnötigen Barrieren, so ein Positionspapier des Bankenverbands.

Als wichtigste Barrieren macht der Bankenverband die Prinzipien der Datensparsamkeit und der Zweckbindung aus. Namentlich die Zweckbindung hält Andreas Krautscheid für überholt, da der Zweckfokus bei modernen Services zunehmend ausfranst. Wenn jedoch jeweils nur die für einen konkreten Zweck benötigten Daten verwendet werden dürfen, dann bedeutet dies im Umkehrschluss, dass Mehrwertservices, die an diesen Zweck andocken könnten, jedes Mal einer erneuten Einwilligung bedürfen.

Die Zweckbindung weiterentwickeln

Der Bankenverband fordert deshalb eine Weiterentwicklung des 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.

Völlig aus der Luft gegriffen sind solche Vorschläge nicht. Als Muster könnten zum Bespiel die „White-Lists" gelten, wie es sie im Kontext der PSD2 gibt, um Erleichterungen in Sachen 2-Faktor-Authentifikation zu schaffen. Ähnlich wie dort etwa Online-Shops, denen ein Kunde vertraut, auf eine solche White-List gesetzt werden können, wäre es vielleicht denkbar, dass Kunden ihrer Hausbank eine Art „Pauschalfreigabe" für die Datenverwendung gewähren könnten, wenn sie davon ausgehen, dass diese damit kein Schindluder treibt.

Angesichts des hohen Vertrauens, dass Banken und Sparkassen genießen, wenn es um Datenschutz geht, könnte dies ein praktikabler Ansatz sein, der neue Mehrwertservices und individualisierte Kundenansprache ermöglicht. Dass Banken eine solche anbieterbezogenen Einwilligungserklärung nicht missbrauchen, wäre allein schon aufgrund des damit verbundenen Imageschadens mehr als unwahrscheinlich, den sich die Branche gar nicht leisten kann. Außerdem könnte der Kunde die Einwilligung natürlich jederzeit widerrufen.

Vorstellbar – aber für den Kunden vermutlich schwieriger – wäre vielleicht auch eine Art Einwilligungserklärung im Baukastensystem, bei der der Kunde seine Einwilligung zu jeweils verschiedenen (auch erweiterten) Zwecken erteilen oder widerrufen kann. In diesem Fall müsste klar und verständlich erklärt werden, worum es bei dem zu setzenden Haken jeweils geht.

Dennoch wäre eine solche Vorgehensweise immer noch praktischer, als die Einwilligungsoptionen jedes Mal aufs Neue abzufragen. Denn bei Online-Prozessen führen Auswahlmöglichkeiten wie „Check-Boxen" mit einer Vielzahl von Optionen zu hohen Abbruchraten, da sie nicht nur zeitraubend sind, sondern zum Teil Entschei-

dungen verlangen, die den Kunden in der jeweiligen Situation leicht überfordern können.

Mehr Verständlichkeit bei der Datenschutzerklärung

Generell gehört damit auch die mit der Einwilligung eng verbundene Datenschutzerklärung auf den Prüfstand. Hier fordert der Bankenverband ein an den Kundenbedürfnissen ausgerichtetes Transparenzkonzept hinsichtlich Datennutzung, um die Datensouveränität des Verbrauchers zu stärken und Vertrauen in die Datenfreigabe für innovative Produkte zu schaffen.

Transparenz bedeutet dabei nicht möglichst ausführliche und in wasserdichtem Juristendeutsch abgefasste Erklärungen, wie sie durch die Datenschutz-Grundverordnung massiv zugenommen haben. Denn diese Informationsflut kann der Kunde gar nicht mehr wahrnehmen beziehungsweise einordnen.

Transparenzstandards entwickeln

Um dem Kunden wirklich die Souveränität über seine Daten zu geben, braucht es deshalb Transparenzstandards, die den Aspekt der Verständlichkeit betonen. Der Bankenverband schlägt dabei sogar vor, mit Symbolen oder Icons zu arbeiten und ein Datenschutzglossar zu erarbeiten, das auf verständliche Weise die datenschutzrechtlich am häufigsten auftretenden Begriffe im Zusammenhang mit Finanzdienstleistungen erläutert.

Außerdem solle der Gesetzgeber zweistufige Informationsvermittlungskonzepte akzeptieren, die in Stufe 1 überblicksartig kurze, prägnante Informationen bieten, die in der zweiten Stufe bei Bedarf durch weitere Detailinformationen ergänzt werden.

Auch hier kann ein anderes Regulierungsfeld als Vorlage dienen: Wenn man beim Produktinformationsblatt auf einen Überblick über die wichtigsten Fakten setzt – warum sollte sich dieses Prinzip nicht auf die Datenschutzerklärung übertragen lassen?

Vorteile der Datenverwendung kommunizieren

Wer auf dieser Basis die Einwilligung seiner Kunden zur Datenverwendung erlangen will, der muss das Thema auch stärker kommunizieren und die Vorteile einer erweiterten und aggregierten Nutzung von Daten erklären. Offensichtliche Vorteile sind eine bessere Beratung auf breiterer Datengrundlage, die Verbesserung in die Zukunft gerichteter Finanzszenarien oder auch die Verhinderung von Betrug.

Es muss jedoch auch deutlich gemacht werden, dass die Datenverarbeitung in bestimmten Fällen schon aufgrund gesetzlicher Vorgaben unabdingbar (Stichworte: verantwortungsvolle Kreditvergabe oder Betrugsprävention) oder aufgrund einer Interessenabwägung zumindest legitim ist (Stichworte: Austausch mit Kreditauskunfteien, Nutzung von Daten zu Werbezwecken).

Steuerbarkeit durch Datenschutzcockpit

Wichtig ist auch, dass der Kunde die Anbieternutzung seiner Daten einfacher und bequemer als bisher steuern kann als bisher. Nur dann kann er die Kontrolle über seine Daten tatsächlich bewusst und souverän auszuüben. 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.

Deshalb plädiert der Bankenverband für ein nutzerfreundliches digitales Datenschutzcockpit, 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 ein solches 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.

Das Datenschutzcockpit könnte im Rahmen einer zentralen Daten-/Identitätsmanagement-Plattform zusammengeführt werden. Sie 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. Bei der Verknüpfung mit einem neuen Dienst könnten Nutzer die Freigabeeinstellungen der Daten einstellen und entscheiden, welche Daten an wen übertragen und zu welchen Anlässen genutzt werden dürfen. Außerdem könnte er den gewünschten Grad an Bequemlichkeit definieren, anhand dessen sich für die jeweiligen Dienste beispielsweise ergibt, ob Kontakt-, Bank- oder Versanddaten automatisch übertragen werden.

Vorbild „Social-Log-In"

Eine Cockpitlösung könnte einerseits von datenverarbeitenden Unternehmen innerhalb des Nutzerprofils bereitgestellt, andererseits aber auch von vertrauensvollen Drittanbietern (Trusted Parties) angeboten

Die Forderungen des Bankenverbands zur Datennutzung

1. Relativierung des Prinzips der Datensparsamkeit, unter anderem 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, 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, das heißt kurze, prägnante Informationen zur Gewährung des Überblicks (Stufe 1) und auf Nachfrage weitere Detailinformationen (Stufe 2).

4. Förderung und Akzeptanz eines modifizierten Transparenzkonzepts durch den Gesetzgeber beziehungsweise 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 beziehungsweise Erläuterung der Symbole oder Icons mit rechtsverbindlicher Wirkung auf Nachfrage beziehungsweise an zentraler Stelle eines Dienstes oder einer Website.

5. Förderung eines konkreten, einheitlichen Standards zur vereinfachten Darstellung von Informationen und „Botschaften" (zum Beispiel Icons, Stichpunkte, One-Pager).

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

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 er 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.

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.

Aus Verbrauchersicht wäre dies vermutlich eine ideale Lösung – analog zu dem zentralen „Vorsorgekonto", das nach den Vorstellungen der Politik Verbrauchern künftig den Gesamtüberblick über die zu erwartenden Altersbezüge geben und dabei die gesetzliche Rente ebenso einbeziehen soll wie die betriebliche Altersvorsorge und – unabhängig vom gewählten Anbieter – die privat getroffenen Vorsorgemaßnahmen. Gar so bald wird das Datenschutzcockpit aber vermutlich keine Realität werden. Dagegen spricht nicht nur die Komplexität, die mit dem Aufbau verbunden wäre. Zuvor müssten auch Rechts- und Haftungsfragen im Fall von Verstößen geklärt werden. Und nicht zuletzt wäre die Finanzierungsfrage zu klären: Soll der Nutzer die Kosten für den Betrieb eines Datenschutzcockpit tragen – etwa in Form von Jahresbeiträgen? Oder müsste die Finanzierung von den Anbietern der entsprechenden Dienste kommen?

Entgelte für die Nutzung seitens der Verbraucher könnten die Akzeptanz solcher Plattformen beträchtlich sinken lassen und damit die Wirtschaftlichkeit infrage stellen. Bei der Erhebung von Entgelten auf der Anbieterseite stellt sich die Frage, ob Unternehmen dann überhaupt solche Plattformen nutzen und nicht lieber doch bei der bisherigen Praxis bleiben würden. Oder wird das Datenschutzcockpit womöglich zu einer hoheitlichen Aufgabe – angesiedelt etwa unter dem Dach des BSI?