

Blog

Post-PSD2: Nutzung von Daten zwischen Kundenmehrwert und Datensouveränität

12.06.2018

von



Beyritz, Ingo

Kurzgefasst

Politik und wirtschaftliche Akteure sollten drei Maßgaben ins Zentrum ihres Handelns stellen, um das Spannungsverhältnis zwischen Mehrwert von Dienstleistungen und Kontrolle über die eigenen Daten aufzulösen: Erstens Mehrwert für den Bürger durch Datennutzung, zweitens adressatengerechte Transparenz bei der Datennutzung und drittens einfache Steuerbarkeit der Datennutzung über ein Datenschutz-Cockpit.

Schlagworte

Zahlungsverkehr

PSD2

Digitalisierung



Die Digitalisierung der Geschäftsprozesse bringt nicht nur Unternehmen, sondern gerade auch den Bürgern viele

Blog

Vorteile: Mithilfe datenbasierter Analysen können ihr Verhalten und damit auch ihre Wünsche und Vorstellungen besser „verstanden“ werden. Unternehmen ist es auf diese Weise möglich, maßgeschneiderte Produkte zum richtigen Zeitpunkt anzubieten und somit einen individuellen Mehrwert zu erzielen.



Abonnieren Sie den Blog Bankenverband!

Zum Abonnement

Gerade das Beispiel der zweiten EU-Zahlungsdiensterichtlinie (PSD2) zeigt, wie stark einerseits das Interesse ist, aus Kontodaten Dienstleistungsangebote abzuleiten und andererseits wie wichtig es ist, dabei dem Bürger die Kontrolle zu ermöglichen, wie Kontodaten weitergegeben und verwendet werden.

Hier sollten Politik und wirtschaftliche Akteure die drei folgenden Maßgaben ins Zentrum ihres Handelns stellen, um das Spannungsverhältnis zwischen Mehrwert von Dienstleistungen und Kontrolle über die eigenen Daten aufzulösen:

1. Mehrwert für den Bürger durch Datennutzung

Dem Bürger kann durch Nutzung seiner Daten wertvoller Mehrwert geboten werden, ohne die Kontrolle über seine Daten oder die Privatsphäre einzuschränken.

Die Digitalisierung ermöglicht neue Wert-schöpfungsansätze, von denen die Bürger in Form von besseren, d.h. qualitativ hochwertigen, schnellen, einfachen und günstigen Produkten und Dienstleistungen profitieren können. Signifikanter Mehrwert entsteht beispielsweise im Zusammenhang mit

- tatsächlichen Kundenbedürfnissen,
- individuellen Produkten und Dienstleistungen,
- dem Schutz des Bürgers vor wirtschaftlichen Verlusten
- und genauerer Risikosteuerung für die Bank.

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

2. 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. Hierzu ist es erforderlich, praxisgerechte Transpa-

Blog

renzkonzepte und Steuerungsinstrumente zu entwickeln und zu implementieren.

Anhand der heutigen Datenschutzerklärungen ist es oftmals kaum möglich ist, einen Einblick in die Verarbeitung personenbezogener Daten zu nehmen. Zusätzlich sollte eine verständliche und einheitliche Symbolik – ähnlich der Lebensmittelampel – Hilfestellung geben. Ein kundengerechtes Transparenzkonzept sollte folglich aus zwei Stufen bestehen:

1. Einfache und verständliche Verbraucherinformation zur Datennutzung, zum Beispiel in Form von Symbolen.
2. Detaillierte Information beziehungsweise Erläuterung der Symbole mit rechtsverbindlicher Wirkung, beispielsweise auf einer Webseite oder auf Nachfrage.

3. Einfache Steuerbarkeit der Datennutzung über ein Datenschutz-Cockpit

Neben einer hinreichenden Transparenz sollte der Bürger die tatsächliche Anbieternutzung seiner Daten einfacher und bequemer als bisher steuern sowie nachvollziehen können. Damit würde er befähigt werden, die Kontrolle über seine Daten bewusst und souverän auszuüben.

In der Praxis ist es für den Einzelnen aufgrund der Vielzahl seiner Vertragspartner und der unterschiedlichen Vertragsverhältnisse kaum möglich, die Übersicht zu behalten, wer seine Daten wofür und in welchem Umfang verarbeiten darf. Ein anbieterübergreifendes Datenschutz-Cockpit würde eine wirksame Kontrolle ermöglichen, wodurch auf einen Blick erkannt und 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 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.

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.