



Universität Augsburg
Prof. Dr. Hans Ulrich Buhl
Kernkompetenzzentrum
Finanz- & Informationsmanagement
Lehrstuhl für BWL, Wirtschaftsinformatik,
Informations- & Finanzmanagement

UNIA
Universität
Augsburg
University

Diskussionspapier WI-210

Widersprüchliche Ziele bei Daten- und Verbraucherschutz?

von

Marcus Kaiser

in: Informatik-Spektrum 31 (2008) 2, S. 151-160

Widersprüchliche Ziele bei Daten- und Verbraucherschutz?

Marcus Kaiser

Der Datenschutz hat zum Ziel, dass Verbraucher über die Verwendung ihrer personenbezogenen Daten selbst bestimmen können. Demgegenüber schreiben neue Verbraucherschutzvorschriften im Bereich der Finanzdienstleistungen die Dokumentation personenbezogener Daten vor und bringen Kunden und Finanzberater somit in ein Dilemma.

daher von den datenschutzrechtlichen Vorschriften betroffen. In jüngerer Zeit erschienen in der Zeitschrift Informatik-Spektrum zwei Beiträge, die sich mit dem Datenschutz befassen. Im ersten nennt Roßnagel [20] u.a. die durch Informationstechnologie ermöglichte Individualisierung als eine von mehreren aktuellen Entwicklungen, aufgrund derer die Verarbeitung personenbezogener Daten in Zukunft weiter zunehmen wird. Im zweiten Beitrag erwähnt Mertens [17] die Tatsache, dass Daten, die im Rahmen eines Fragebogens gemäß des Wertpapierhandelsgesetzes (WpHG) über den Kunden erhoben werden, zur Beratung hinsichtlich einer anderen Finanzdienstleistung nicht verwendet werden dürfen.

Der vorliegende Beitrag hat – angeregt durch die Ausführungen der beiden genannten Artikel –

Einleitung¹

Seit mehreren Jahren wird im Finanzdienstleistungssektor die Individualisierung von Beratungsleistungen mithilfe von Informationstechnologie als Mittel zur Differenzierung im Markt gefordert [4]. Sie setzt die Erhebung, Verarbeitung und Speicherung von kundenbezogenen Daten voraus und ist

zum Ziel, die unterschiedlichen Facetten der Vorschriften zum Umgang mit Kundendaten im Bereich der individualisierten Beratung im Finanzdienstleistungssektor zu analysieren. Dabei werden die Konflikte zwischen Vorschriften des Datenschutzes und neu erlassenen Vorschriften zur Dokumentation im Rahmen der privaten Finanzplanung diskutiert. Es folgen Herausforderungen, denen sich Finanzdienstleister aktuell gegenüber gestellt sehen, und mögliche Lösungswege, die die Informatik bietet.

Begriffe

Der Begriff der *privaten Finanzplanung* (engl. financial planning) wird definiert als „[...] ganzheitliche Beratungsdienstleistung, die als ein systematisch koordinierter Planungsprozess – bestehend aus Akquisition/Kontaktaufnahme, Auftragsvergabe, Datenaufnahme, Analyse und Planung, Dokumentation, Betreuung mit Realisierung und periodische Kontrolle – organisiert ist.“ [27]. Der Begriff „ganzheitlich“ aus obiger Definition bezieht sich auf sämtliche Finanzdienstleistungen für Privatkunden, wovon für den vorliegenden Beitrag speziell Versicherungen und Wertpapiere relevant sind, da diese im Fokus der betrachteten EU-Richtlinien zum Verbraucherschutz stehen.

Als *Versicherungsvermittlerrichtlinie* (VVR) wird das Gesetz zur Neuregelung des Versiche-

¹ Der Autor dankt Prof. Dr. H.U. Buhl und Prof. Dr. Dr. h.c. mult. P. Mertens für wertvolle Anregungen.

Zusammenfassung

Der Datenschutz ist ein immer wieder neu diskutiertes Thema. Sein grundlegendes Ziel ist, dass der Bürger selbst über seine personenbezogenen Daten bestimmen kann. Für Unternehmen, die zur Unterstützung des Kundenkontakts Informationssysteme einsetzen, besteht daher bereits die Herausforderung, von ihren Kunden die Einwilligung zur automatisierten Verarbeitung deren personenbezogener Daten einzuholen. Der Artikel stellt dar, wie neue Vorschriften im Bereich des Verbraucherschutzes bei Finanzdienstleistungen (Vermittlerrichtlinie und MiFID (engl. Markets in Financial Instruments Directive)) nun sogar vorschreiben, dass bestimmte personenbezogene Daten des Kunden zu dokumentieren sind. Es wird erläutert, weshalb hierdurch Kunde und Finanzberater in ein Dilemma geraten und welche Herausforderungen sich für Finanzdienstleister bzgl. des Umgangs mit Kundendaten aufgrund dieser Vorgaben ergeben. Zudem werden resultierende Fragestellungen für die Informatik diskutiert.

rungsvermittlerrechts bezeichnet, das die EU-Richtlinie über Versicherungsvermittlung in deutsches Recht implementiert. *MiFID* steht für das Finanzmarkt-Richtlinie-Umsetzungsgesetz, das in Deutschland die EU-Richtlinie über Märkte für Finanzinstrumente in nationales Recht umsetzt.

(Finanz-)Berater bezeichnet im Folgenden eine Person, welche die Dienstleistung der privaten Finanzplanung erbringt. Tut sie dies ganzheitlich, so ist sie von den Vorschriften aus der VVR und der MiFID insofern betroffen, als sie dann i.d.R. als gewerbsmäßiger Versicherungsvermittler oder Versicherungsberater im Sinne der VVR agiert und die Tätigkeiten der Anlageberatung und der Anlagevermittlung im Sinne der MiFID erbringt.

Als *Individualisierung* bezeichnet man in Anlehnung an [18] sowohl die Anpassung einer Leistung – in unserem Fall die private Finanzplanung – an die Eigenschaften, Bedürfnisse und Kenntnisse einer Person – in unserem Fall des Kunden – als auch die Anpassung der Leistung an die Rechte und Pflichten der Person.

Gestaltungsmöglichkeiten im Datenschutz

Der Datenschutz erachtet die Verarbeitung von personenbezogenen Daten nur dann als zulässig, wenn der Gesetzgeber oder der Betroffene diese hinsichtlich Umfang und Zweck gebilligt hat [20].

In der Praxis wird diese Billigung durch den Betroffenen zumeist in Form einer datenschutzrechtlichen Einwilligung eingeholt. Dies geschieht überwiegend mit Bezug auf einen spezifischen Anlass (z.B. Anmeldung bei einem Internetportal, Kauf eines Produktes). Damit geht i.d.R. einher, dass sich die Zustimmung hinsichtlich Umfang und Zweck an dem spezifischen Anlass, im Rahmen dessen sie eingeholt wird, orientiert (*anlassspezifische Einwilligung*). Dadurch wird dem im Datenschutz geltenden Prinzip der Erforderlichkeit Genüge getan. Dieses wird konkretisiert durch die Prinzipien Datenvermeidung und Datensparsamkeit („Verarbeite keine“ bzw. „Verarbeite so wenig wie möglich Daten“ [20, 28]). Diese anlassorientierte Vorgehensweise führt zu anfangs genanntem Sachverhalt, den Mertens [17] in seinem Beitrag kritisiert: Personenbezogene Daten eines Kunden, die im Rahmen eines Fragebogens gemäß WpHG spezifisch zu diesem Anlass erhoben wurden, dürfen nicht für andere Zwecke verwendet werden. Dies gilt auch dann, wenn aus diesen Daten ersichtlich wird, dass für den Kunden der Kauf einer anderen Finanzdienstleistung (bei Mertens eine Riester-Rente) sinnvoll ist. Er sieht darin ein Beispiel dafür, dass der Datenschutz Unternehmen daran hindert, dem Kunden Produktvorschläge zu unterbreiten, die für ihn sinnvoll wären.

Jedoch ist eine derartige Verarbeitung gesetzlich keineswegs grundsätzlich ausgeschlossen. Vielmehr haben Unternehmen die Möglichkeit, sich datenschutzkonform die Einwilligung des Kunden hierzu einzuholen: Aus rechtlicher Sicht spricht nichts dagegen, Zweck und Umfang in der Einwilligung so zu spezifizieren, dass die erhobenen Daten zur Beratung des Kunden bei anderen Anlässen genutzt werden können (*anlassübergreifende Einwilligung*). Hiervon profitieren im Idealfall sowohl der Kunde als auch das Unternehmen. Selbstverständlich sind hierbei die formalen Anforderungen des Datenschutzes an die Einwilligung [23, 31] zu berücksichtigen. Zu beachten ist vor allem, dass eine „Generalvollmacht“ rechtlich nicht zulässig ist, sondern Zweck und Umfang explizit definiert werden müssen [23]. Im Beispiel von Mertens bedeutet

Abstract

Privacy is a topic heavily discussed. The basic aim of regulation related to privacy is to enable the citizen to control information about his person. Firms that use information systems for supporting customer relationship management therefore face the challenge to obtain an approval by their customers for automatically processing personal data. This article describes in what way new regulations concerning consumer protection in the financial services sector prescribe the documentation of customers' personal data. It is illustrated for what reasons customers and financial consultants get into a dilemma. Moreover, the article states new challenges for financial services providers resulting from these regulations. In addition, questions related to informatics are discussed.

dies, den Zweck der Datenerhebung nicht auf die Risikoeinschätzung des Kunden für den Wertpapierhandel zu beschränken. Stattdessen müssen die Unternehmen sämtliche Anlässe antizipieren, in denen die abgefragten Daten zur Beratung des Kunden verwendet werden können, und diese in die Zweck- und Umfangbestimmung der Einwilligung einschließen. Möchte ein Unternehmen, dass ein Kunde in eine derartige Verwendung seiner Daten einwilligt, muss es bereit sein, Zusatzaufwand zu leisten und den Kunden detailliert über das beschriebene Vorgehen und den damit verbundenen Nutzen zu informieren. Damit verhält sich das Unternehmen gesetzeskonform: „Wird der Betroffene ernst genommen, informiert und um Zustimmung in Form einer Einwilligung oder eines Vertrages gebeten, ist die Verarbeitung personenbezogener Daten zum Zweck der Personalisierung datenschutzrechtlich kein Problem.“ [21].

Wenn es aber möglich ist, durch Zustimmung des Kunden die rechtliche Grundlage für eine über einen konkreten Anlass hinaus gehende Verarbeitung seiner Daten zu schaffen, stellt sich die Frage, warum dies in der Praxis kaum erfolgt. Folgende Gründe lassen sich hierzu anführen:

1. Wenn sich Unternehmen einen Fehler im Umgang mit dem Datenschutz oder der Datensicherheit leisten, wird in den Medien darüber

berichtet [14, 15]. Dies kann einen erheblichen Ansehensverlust nach sich ziehen. Die Gefahr hierzu besteht auch dann, wenn Unternehmen zwar im beschriebenen Sinne legal handeln, aber Datenschützer das Vorgehen öffentlich kritisieren. Dies hat zur Folge, dass Unternehmen im Bezug auf den Datenschutz überaus (und teilweise über-)vorsichtig reagieren statt agieren.

2. „Unnötige Bürokratie ist ein Bremsklotz für jede wirtschaftliche Betätigung. Sie kostet Zeit und Geld und davon haben gerade kleine Unternehmen nichts zu verschenken.“ [6]. So wird Bundeswirtschaftsminister Glos bzgl. des Entwurfs eines Gesetzes zum Abbau bürokratischer Hemmnisse zitiert. Hierbei ist geplant, die Pflicht zur Bestellung von Datenschutzbeauftragten auf Unternehmen zu reduzieren, die mindestens zehn (bisher fünf) mit Personendatenverarbeitung betraute Mitarbeiter beschäftigen. Dass Datenschutzbeauftragten dieses Bild des Bremsklotzes anhängt, resultiert auch aus der in der Praxis verbreiteten Vorgehensweise, in welcher der Datenschutzbeauftragte eine Spezifikation mit der Bitte um Prüfung vorgelegt bekommt. Häufig wählt er nur zwischen zwei Möglichkeiten: Entweder die Spezifikation als datenschutzkonform zu akzeptieren oder sie abzulehnen. Akzeptiert er gewisse Risiken, geht er ein persönliches Risiko ein. Er wird dieses daher zumindest benennen, zumal er an dem zugehörigen Ertrag i.d.R. nicht beteiligt ist. Nach Alternativen, wie das Vorhaben dennoch umgesetzt werden könnte, wird er meistens nicht gefragt. Er bietet solche aber auch nur selten aus Eigeninitiative an. Lehnt er die Spezifikation ab, gilt er als der verneinende Bedenkenräger und verfestigt das zitierte Bild. Unternehmen, die derartiges Verhalten ihrer Datenschutzbeauftragten akzeptieren oder gar fördern, können von diesen keine Innovationen erwarten.
3. Es besteht dahingehend Unsicherheit, inwieweit Kunden eine veränderte Vorgehensweise seitens der Unternehmen bzgl. des Datenschutzes von der Erfüllung einer leidigen Pflicht hin zu einem gestaltbaren Vertragsgegenstand akzeptieren. Aus existierenden Studien kann die Frage, ob ein derartiges Vorgehen von Kunden akzeptiert oder abgelehnt wird, nicht eindeutig beantwortet werden. So äußern sich Kunden in Deutschland sehr datenschutzbewusst [19]. Studien (v.a. im

Bereich des E-Commerce) legen aber den Schluss nahe, dass die Äußerung von Datenschutzbewusstsein nicht immer auch ein entsprechendes Verhalten nach sich zieht: Vielmehr stellen auch Kunden, denen der Schutz ihrer Privatsphäre sehr wichtig ist, im Internet ohne zwingenden Grund ihre persönlichen Daten zur Verfügung [2]. Die aktuellen Verhaltensweisen von Nutzern im Bereich Web 2.0 bestätigen dies [12]. Zudem kommen Untersuchungen zu dem Schluss, dass Kunden, die ihre Daten nicht preisgeben wollen, nicht grundsätzlich keine Daten weitergeben möchten. Neben dem Vertrauen in das jeweilige Unternehmen wird die Bereitschaft der Kunden, persönliche Daten zur Verfügung zu stellen, stark durch die wahrgenommene Gegenleistung des Unternehmens für die Weitergabe ihrer Daten beeinflusst [7, 29].

Die genannten Punkte stehen einer anlassübergreifenden Einwilligung entgegen und lassen sich nur durch einen Einstellungswandel der jeweils beteiligten Akteure überwinden. Unternehmen dürften am ehesten im Bereich des dritten Punkts dazu gezwungen werden, ihre Einstellung zum Thema Datenschutz zu überdenken. Zum einen illustrieren die zitierten Untersuchungen, dass Kunden der Preisgabe ihrer Daten durchaus positiv gegenüber stehen, sofern sie eine Gegenleistung erkennen. Zum anderen dürften die immer anspruchsvolleren Kunden [13] verstehen, dass Anbieter nur auf Basis ihrer persönlichen Daten ihre Bedürfnisse nach Leistungen, die auf sie zugeschnitten sind, angemessen befriedigen können. Daher müssen Unternehmen über kurz oder lang alternative Wege zum bisherigen defensiven Umgang mit dem Thema Datenschutz beschreiten.

Daten- und Verbraucherschutz in der privaten Finanzplanung

Banken und Versicherungen sind seit kurzem gesetzlich dazu verpflichtet, den bisherigen Umgang mit Kundendaten zu überdenken. Für sie schafft der Gesetzgeber ein Dilemma zwischen Daten- und Verbraucherschutz: Gemäß der beiden EU-Richtlinien VVR und MiFID müssen personenbezogene Daten über den Kunden erhoben und dokumentiert werden. Im Folgenden wird daher zunächst kurz erläutert, weshalb der Datenschutz im Bereich der privaten Finanzplanung eine Rolle spielt. Es

folgen der Inhalt der beiden Richtlinien und eine Darstellung, weshalb diese aus Sicht des Autors in einem Widerspruch zum Datenschutz stehen. Den Abschluss bilden Überlegungen, wie Unternehmen diesen Herausforderungen kundenorientiert begegnen können.

Relevanz des Datenschutzes in der privaten Finanzplanung

Zum einen basiert eine individualisierte Beratung in der privaten Finanzplanung notwendigerweise auf Informationen über den Kunden – also auf personenbezogenen Daten. Zum anderen erlaubt es speziell im Massenkundengeschäft erst der Einsatz von Informationssystemen, individualisierte Beratungsdienstleistungen wirtschaftlich anzubieten. Hierbei werden personenbezogene Daten automatisiert verarbeitet. Somit ist eine Auseinandersetzung mit den datenschutzrechtlichen Bedingungen im Bereich der individualisierten privaten Finanzplanung notwendig.

Dokumentation personenbezogener Daten aufgrund gesetzlicher Vorschriften

Wie bereits erwähnt, ist eine Verarbeitung personenbezogener Daten erlaubt, wenn der Gesetzgeber sie billigt. Für die private Finanzplanung existieren keine speziellen derartigen Vorschriften. Implizit wird aber eine solche Verarbeitung personenbezogener Daten im Bereich der individualisierten privaten Finanzplanung aus folgendem Grund verlangt: Seit Jahren wird die Qualität von Finanzdienstleistungsberatungen regelmäßig als mangelhaft bewertet. Jüngstes in einer langen Reihe von Beispielen [13, 24] ist ein Beitrag der Zeitschrift Finanztest zu Beratungen im Kreditbereich [26]. Die schlechte Qualität liegt oftmals auch an der Qualifikation der Berater: So ist deren Leistung einer Studie zufolge in jedem zweiten Fall nur mittelmäßig und ca. in jedem dritten Fall schwach [22]. Vor allem im Massenkundengeschäft kann in vielen Fällen von einem „systematisch koordinierten Planungsprozess“ kaum die Rede sein. Stattdessen wird häufig beklagt, dass die vorherrschende Entlohnungspraxis auf Umsatzbasis den provisionsgetriebenen Produktverkauf fördert, aber „kaum Anreize für eine qualitativ hochwertige Anlageberatung [bietet].“ [13]. Vor diesem Hintergrund erließ der Gesetzgeber die beiden bereits genannten Vorschriften zur Verbesserung des Verbraucherschutzes in der privaten

Finanzplanung, VVR und MiFID. Dort schreibt er einen in der Theorie eigentlich obligatorischen, in der Praxis aber offensichtlich kaum durchgeführten Vorgang als verpflichtend vor: Die Dokumentation der einzelnen Prozessschritte der privaten Finanzplanung. Um das Spannungsfeld zwischen den Zielsetzungen des Datenschutzes und diesen beiden EU-Richtlinien darzustellen, werden im Folgenden die Auswirkungen der beiden Richtlinien auf die Verarbeitung personenbezogener Daten analysiert.

Versicherungsvermittlerrichtlinie

Die „Richtlinie des Europäischen Parlaments und des Rates über Versicherungsvermittlung“ wurde am 9. Dezember 2002 verabschiedet. Das Gesetz zur Neuregelung des Versicherungsvermittlerrechts setzt diese in deutsches Recht um und ist zum 22. Mai 2007 in Kraft getreten. In Deutschland betrifft sie ca. 500 000 Vermittler [16]. Die VVR schreibt vor, die Wünsche und Bedürfnisse des Kunden sowie die Gründe für den erteilten Rat festzustellen, zu dokumentieren und die Dokumentation an den Kunden auszuhändigen. Im Falle von Beratungsfehlern, die auf eine Verletzung dieser Verpflichtungen zurückzuführen sind, hat der Kunde Anspruch auf Schadensersatz durch den Berater.

Wie bereits angedeutet, liegen die Berührungspunkte der VVR zum Datenschutz in den zu dokumentierenden Informationen über den Kunden. Da der Gesetzgeber weder bei den Wünschen und Bedürfnissen des Kunden noch bei den Gründen für den erteilten Rat exakt vorschreibt, wie diese zu dokumentieren sind, werden diese Berührungspunkte nicht auf den ersten Blick deutlich. Dass es sich aber bei den zu dokumentierenden Informationen in den meisten Fällen um personenbezogene Daten handelt, verdeutlicht das folgende Beispiel: Ein Kunde sucht seinen Berater auf, da er für seine Mietwohnung eine Hausratversicherung abschließen möchte. Eine Faustregel besagt, dass die Versicherungssumme mithilfe der Formel *Fläche der Wohnung (in m²) × 650 EUR* festzulegen ist. Diese Formel genügt nicht den Ansprüchen einer Individualisierung, da es viele Fälle gibt, in denen ihre Anwendung zu einer Unter- bzw. Überdeckung führt [5]. Dennoch soll sie hier zur Veranschaulichung vereinfachend als geeignet angenommen werden. Dann muss der Berater die Formel (als Grundlage für die Bedürfnisermittlung) und das in sie eingehende personenbezogene

Datum (die Quadratmeterzahl der Wohnung des Kunden) der Logik der VVR folgend als Begründung dokumentieren.

Bereits dieses einfache Beispiel veranschaulicht, dass bei der Dokumentation sowohl der Ermittlung der Wünsche und Bedürfnisse als auch der Begründung des erteilten Rats personenbezogene Daten verarbeitet werden. In der Realität gestaltet sich eine Individualisierung wesentlich komplexer. Dies verdeutlichen die von verschiedenen Organisationen erarbeiteten Vorlagen zur Dokumentation: Für den im Beispiel betrachteten Fall einer Hausratversicherung wird z.B. empfohlen, über 25 Angaben des Kunden einzuholen und zu dokumentieren (z.B. „War Ihr Hausrat in den letzten fünf Jahren von Schäden betroffen?“, „Ist die Wohnung länger als 60 Tage ununterbrochen unbewohnt?“ [1]). Wie oben erwähnt, sind hierbei in der Regel Informationssysteme beteiligt.

Die VVR problematisiert die Tatsache, dass die Dokumentation – wie illustriert – im Widerspruch zum Datenschutz steht, nicht. Daher ist den Beratern dieser Widerspruch oft nicht bewusst, er wird in der praxisorientierten Literatur nach Kenntnis des Autors nur am Rande angesprochen [30]. Zudem macht die VVR keine konkreten Vorgaben bzgl. der tatsächlich abzufragenden personenbezogenen Daten. Somit werden die vom Gesetzgeber im Unklaren gelassenen Berater, die sich vor Schadensersatzforderungen schützen wollen, im Zweifelsfall eher zu viele als zu wenige Daten abfragen und dokumentieren. Dies steht wiederum im Widerspruch zu den im Datenschutz geltenden, oben erwähnten Prinzipien der Datenvermeidung bzw. der Datensparsamkeit.

Aber nicht nur der Berater, auch der Kunde gerät in ein Dilemma: Ist ihm daran gelegen, seine Daten nicht für die Dokumentation preiszugeben, muss er nicht nur auf eine qualitativ hochwertige Beratung verzichten, da eine solche auf eine gute Datenbasis angewiesen ist. Zudem muss der Kunde gemäß VVR eine Erklärung unterzeichnen, die ihn ausdrücklich darauf hinweist, dass er mit seiner Unterschrift auf Schadensersatzansprüche gegenüber dem Berater verzichtet. Bei der Abwägung zwischen den beiden Möglichkeiten werden sich Kunden in vielen Fällen gegen ihr Recht auf Datenschutz und zugunsten des Schadensersatzanspruchs bei einer Falschberatung entscheiden, ein Verhalten, das auch die Stiftung Warentest empfiehlt [25]. Auch

Vertreter der Versicherungspraxis raten Beratern, die Verzichtserklärung nur in Ausnahmefällen einzusetzen [9].

Richtlinie über Märkte für Finanzinstrumente

Nicht nur im Bereich der Versicherungen, auch bei Wertpapieren zielt der Gesetzgeber auf eine Verbesserung des Verbraucherschutzes ab. Zu diesem Zweck verabschiedeten das Europäische Parlament und der Rat 2004 die „Richtlinie über Märkte für Finanzinstrumente“ (MiFID). Das Gesetzgebungsverfahren in Deutschland wurde im Mai 2007 abgeschlossen, das Gesetz trat am 1. November 2007 in Kraft. Die MiFID definiert drei Dienstleistungstypen (Portfolioverwaltung und Anlageberatung, beratungsfreie Finanzdienstleistungen, reines Ausführungsgeschäft [8]), für die sie vorschreibt: „Eine Wertpapierfirma sorgt dafür, dass Aufzeichnungen über alle ihre Dienstleistungen und Geschäfte geführt werden, die ausreichen, um der zuständigen Behörde zu ermöglichen, die Einhaltung der Anforderungen dieser Richtlinie zu überprüfen und sich vor allem zu vergewissern, dass die Wertpapierfirma sämtlichen Verpflichtungen gegenüber den Kunden oder potenziellen Kunden nachgekommen ist.“ Unter diese Dokumentationspflicht fällt auch die Anforderung der MiFID, dass Berater bei der Anlageberatung – als Teilgebiet der privaten Finanzplanung – Informationen über die Kenntnisse und Erfahrungen des Kunden sowie über seine finanziellen Verhältnisse, Verpflichtungen und Anlageziele einholen müssen [8]. Auch wenn bislang für die MiFID noch keine Dokumentationsempfehlungen erarbeitet wurden, ist abzusehen, dass zur Erfüllung dieser Anforderungen personenbezogene Daten des Kunden zu verarbeiten sind. Somit ist also auch bei Wertpapieren eine Dokumentationspflicht gegeben, die in einem ähnlichen Widerspruch zum Datenschutz steht wie dies oben bei der VVR diskutiert wurde.

Zusammenfassend lässt sich sagen, dass die MiFID mit dem Datenschutz in ähnlicher Weise konfligiert wie die VVR, ohne dass dies in einer der beiden Vorschriften thematisiert wird. Es kann nicht davon ausgegangen werden, dass für VVR und MiFID der Datenschutz keine Rolle spielt, da eine Einschränkung des Datenschutzes einer expliziten Rechtsvorschrift bedarf [31], die in beiden Fällen nicht gegeben ist. Der Gesetzgeber ist aufgefordert,

die Widersprüche, die er hier schafft, zu klären. In der Praxis zeichnet sich folgendes Vorgehen ab: Datenschutz, VVR und MiFID werden als regulatorische Pflicht aufgefasst, die es zu erfüllen gilt. Hierauf weist die Tatsache hin, dass die Vorlagen zur Dokumentation nach VVR eine vom Kunden zu unterzeichnende Datenschutzerklärung enthalten. Dabei bietet eine weitere Vorgabe der MiFID einen Ausweg aus dem Dilemma: Sie verlangt, dass Berater und Kunde bei Aufnahme der Geschäftsbeziehung eine Rahmenvereinbarung abschließen. Bei deren Gestaltung besteht Spielraum, eine anlassübergreifende Einwilligung als Grundlage für eine individualisierte private Finanzplanung zu erreichen.

Umgang mit Kundendaten in der privaten Finanzplanung

Die neuen Verpflichtungen zur Dokumentation und zum Abschluss einer Rahmenvereinbarung in Verbindung mit den bestehenden Datenschutzvorschriften zwingen Unternehmen dazu, die Beziehung zum Kunden auf eine neue vertragliche Grundlage zu stellen.

Somit stehen die Unternehmen vor der Herausforderung, ein Konzept zu entwickeln, in dem für verschiedene Anlässe des Kundenkontakts (z.B. Kontaktaufnahme, Beratung, Produktverkauf) festgelegt ist, wie jeweils Zweck und Umfang der Datenverarbeitung, in die der Kunde dabei einwilligen muss, zu gestalten sind. Der Grundstein hierzu kann in der oben erwähnten Rahmenvereinbarung nach MiFID gelegt werden. Die Relevanz derartiger Überlegungen wird noch deutlicher, wenn man bedenkt, dass der Kundenkontakt gerade bei Finanzdienstleistern nicht ausschließlich über einen Berater, sondern häufig über unterschiedliche Kanäle (z.B. Callcenter, WWW, SB-Automaten) erfolgt. Da bei der Kommunikation über die einzelnen Kanäle ebenfalls die rechtlichen Anforderungen einzuhalten sind, ist ein unternehmensweit einheitlicher Standard unabdingbar.

Die Etablierung eines derartigen Konzepts reicht jedoch i.d.R. nicht aus. Vielmehr muss es (wie oben bereits erwähnt) dem Berater gelingen, das Vertrauen des Kunden zu gewinnen, ansonsten wird dieser nicht bereit sein, die Daten weiterzugeben. Dies erreicht der Berater hauptsächlich dadurch, Mehrwert für den Kunden zu stiften, sodass dieser aus der Weitergabe seiner Daten einen Nutzen erfährt. Dadurch wird er im weiteren Verlauf der

memIQ – eine Idee, die ihrer Zeit voraus war?

Prof. Dr. Hans-Gert Penzel, ehem. Aufsichtsratsvorsitzender der memIQ (heute Generaldirektor, DG-IS, Europäische Zentralbank)

Der im Artikel „Widersprüchliche Ziele bei Daten- und Verbraucherschutz?“ angesprochene elektronische Tresor memIQ ist nach wie vor eine attraktive Idee, die sowohl den Endkunden als auch den Dokumente einstellenden Unternehmen erheblichen Nutzen bringen würde, also eine echte win-win-Situation schaffen könnte:

Aus Endkundensicht wird ein komplettes, vorstrukturiertes Archivsystem zur Verfügung gestellt. Alle Kategorien (Bank, Versicherung, Steuer, Haus/Wohnung, Kommunikation, Autos, Auto, Reisen, etc.) sind geordnet vorstrukturiert und werden ab erstmaliger (und einmaliger) Autorisierung eines Zulieferers mit den Dokumenten dieses Zulieferers befüllt. Dokumente der verschiedenen Geschäftspartner fließen dann jeweils aktuell, zuverlässig und ohne Zusatzaufwand ein. Ab diesem Zeitpunkt sind die Dokumente dann in der Verfügungsgewalt des Endkunden, und er kann über die Verwendung seiner personenbezogenen Daten bestimmen. Durch das XML-Format kann parallel zur unveränderlichen auch eine weiterverarbeitbare Variante zur Verfügung gestellt werden, auf Basis derer der Endkunde zum Beispiel verschiedenste integrierte Auswertungen durchführen kann. Auch hätte memIQ selbst verschiedene Auswertungen angeboten (gegen Mehrpreis).

Aus Sicht der Dokumente einstellenden Unternehmen wird ein einheitliches Versandsystem zur Verfügung gestellt, also eine elektronische Alternative zur gelben Post oder zu einem eigenen elektronischen Verteilsystem. Dies ist kostengünstig hinsichtlich Erstinvestition (es wird kein volles System, sondern nur eine elektronische Schnittstelle benötigt) und im Betrieb (Kosten wesentlich niedriger als Versandkosten). Auch ohne Einschreiben wird die Lieferung verbindlich dokumentiert. Darüber hinaus kann dies eine attraktive Plattform sein, um Zusatzangebote zu platzieren.

Das Ganze funktioniert allerdings nur, wenn sich erhebliche Netzwerkeffekte schaffen lassen,

also relativ schnell eine Vielzahl von Nutzern und zumindest einige grosse Dokumente-Einsteller aktiviert werden können.

Aus meiner Sicht gibt es für das Scheitern drei zusammenwirkende Gründe:

1. Primär haben die Dokumente-Einsteller nicht mitgezogen. Zum damaligen Zeitpunkt war der „Besitz des Endkunden“ die dominierende Maxime. Die Firmen hatten offensichtlich Angst, die Kunden zu verlieren, wenn sie deren Daten über eine dritte Partei als Verteiler laufen lassen oder wenn sie – weil ja Konkurrenten in der gleichen Ablagestruktur vertreten sein können – für den Kunden zu viel Transparenz im Quervergleich schaffen. Die Hürde wäre vielleicht eher überwindbar gewesen, wenn die Preise noch attraktiver gewesen wären – siehe Punkt 3. Heute wäre die Hürde wohl insgesamt niedriger, da klar geworden ist, dass ein ausschliesslicher Besitz des Endkunden unrealistisch ist.

2. Die Zahl der Nachfrager hat nicht schnell genug die kritische Masse erreicht. Die ersten Nachfrager äusserten sich sehr positiv (z.B. solche, die das System für die Hypovereinsbank-Kontoauszüge nutzten). Aber der nötige Mund-zu-Mund- oder E-Mail-zu-E-Mail-Propagandaeffekt war noch nicht stark genug. Wir hatten die weitere Furcht, dass Nachfrager Akzeptanzprobleme entwickeln, weil die Dokumente nicht auf dem Home-PC, sondern im Netz stehen. Diese Angst hätte sich wohl mit dem heutigen Erfahrungsstand nicht bestätigt.

3. Die Kosten der memIQ als eigenständiger AG waren zu hoch. Hätte man das Produkt als Zusatzleistung in einem bestehenden Portal angeboten (z.B. in T-Online, MSN, AOL, Google, Yahoo, ...), hätte man zu Grenzkosten und damit günstiger operieren können. Dann hätte man vermutlich auch lange genug durchhalten können, um die kritische Masse aufzubauen.

Angesichts der inzwischen gemachten Erfahrungen auf allen Seiten wäre es durchaus prüfenswert, ob die Idee heute nicht erfolgreich realisiert werden könnte. Das zunehmend attraktive Angebot von Bürosoftware-Funktionalität als Service im Netz deutet in diese Richtung. Denn hinter der Bearbeitung von Dokumenten fehlt dann letztlich nur noch die geordnete Ablage.

Beziehung weniger Hemmungen haben, seine Daten preiszugeben.

Herausforderungen für die Informatik

Im Rahmen eines neu zu gestaltenden Umgangs mit Kundendaten ergeben sich auch Herausforderungen für die Informatik: Zum einen, wie der Datenaustausch zwischen Kunde und Berater gestaltet wird, und zum anderen, wie sichergestellt werden kann, dass die Dokumentation fehlerfrei ist.

Die Weitergabe von Daten durch den Kunden an den Finanzdienstleister kann durch geeignete Standards wie bspw. P3P [10] einfach und sicher gestaltet werden. Auf Basis eines Standards wie P3P könnte jedoch dem Kunden veranschaulicht werden, welche (weiteren) Datenfelder er an den Finanzdienstleister weitergeben müsste, um hinsichtlich eines bestimmten Produkts ideal beraten werden zu können. Der Kunde bliebe aber weiterhin Herr über seine Daten, da er die Möglichkeit hat, der Weitergabe nur dann zuzustimmen, wenn er sich den entsprechenden Mehrwert durch die jeweilige Beratung verspricht. Eine derartige zentrale Vorhaltung von persönlichen Daten und Dokumenten war Geschäftsmodell des – inzwischen eingestellten – kostenfreien Dienstes *memIQ* (siehe hierzu auch die Ausführungen von Hans-Gert Penzel): Hier war es dem Kunden möglich, alle persönlichen Dokumente in einem „virtuellen Tresor“ online aufzubewahren und bei Bedarf abzurufen und weiterzugeben [11]. Durch diese integrierte Sicht auf Daten und Dokumente des Kunden sollten ihm gezielter Zusatzservices angeboten werden können, als dies bei einer partiellen Sicht – wie sie heute zumeist vorherrscht – möglich ist. Unabhängig davon, ob die personenbezogenen Daten bzw. Dokumente beim Kunden selbst oder bei einem Dritten liegen, hätte deren zentrale Haltung Vorteile. Derartige Formen werden aber nur auf Akzeptanz stoßen, wenn eine entsprechende Möglichkeit zum standardisierten Datenaustausch gegeben ist. Von Seiten der Kunden ist – vor dem Hintergrund der im Beitrag geführten Diskussion – der einfache, sichere und von ihm selbst bestimmte Austausch von Daten entscheidend. Für die Unternehmen ist es zudem wichtig, dass diese Standards an die Daten- und Dokumentenbedürfnisse unterschiedlicher Branchen anpassbar sind. Da zudem durch die Verwendung solcher Angebote auch die Sensitivität von Kunden und Unternehmen bzgl. des Umgangs mit Daten erhöht werden dürfte, ist die

Informatik aufgerufen, diese bestehenden Konzepte weiterzuentwickeln.

Die andere Herausforderung liegt in der Tatsache, dass die Dokumentation jederzeit korrekte Angaben über den Kunden, die von ihm gekauften Produkte und die in diesem Zusammenhang durchgeführte Beratung enthalten muss (siehe [3, S. 164]). Diese Anforderung stellt viele Finanzdienstleister aktuell vor Probleme: Deren Informationssysteme sind häufig an den Anforderungen zum Management von einzelnen Produktgruppen ausgerichtet, sodass die Daten eines Kunden im Informationssystem zu verschiedenen Produkten redundant abgelegt sind. Die sich hieraus ergebende Inkonsistenz wird verstärkt durch die Tatsache, dass oftmals auch für jeden Kanal, über den ein Kundenkontakt erfolgt, eine eigene Datenhaltung durchgeführt wird. Diese Charakteristika von Informationssystemen erschweren eine konsistente und fehlerfreie Dokumentation. Denn stellt der Kunde fest, dass in der Dokumentation Angaben fehlen oder gar falsch sind, wird zumindest sein Vertrauen empfindlich gestört. Kommt es zu einem Rechtsstreit, kann ein Finanzdienstleister viel Geld verlieren, falls eine fehlerhafte Angabe den Kunden begünstigt. Noch mehr Reputation wird verspielt, wenn eine fehlerhafte Angabe den Finanzdienstleister begünstigt. Unternehmen stehen daher vor der Herausforderung, über alle Produkte und Kanäle hinweg auf Basis redundanzfreier Kundendaten zu operieren. Technische Lösungen bestehen bspw. im Master-Data-Management: Bislang bezogen Data-Warehouses häufig lediglich Daten aus operativen Quellen, aggregierten und stellten diese gemäß bestimmter Zwecke dar. Derzeit gehen die Überlegungen dahin, diese Funktionsweise künftig zu erweitern, sodass bei Aktualisierungen im Data-Warehouse die zugrunde liegenden operativen Systeme ebenfalls auf den aktuellen Stand gebracht werden (Retraktion). Die aktuell notwendigen Projekte zur Erfüllung der Anforderungen aus VVR und MiFID wären eine Gelegenheit, derartige Überlegungen in die Praxis umzusetzen und dadurch einen Schritt in die Richtung der Vision eines – mit vielen Vorteilen verbundenen – kundenzentrierten Informationssystems zu tun.

Fazit und Ausblick

Der Artikel illustriert, dass nicht nur das von Mertens beschriebene Ungleichgewicht im Datenschutz

existiert, sondern dass Datenschutz und andere Verbraucherschutzvorschriften im Widerspruch zueinander stehen. Zudem wurde veranschaulicht, dass sich Unternehmen künftig neue Vorgehensweisen bzgl. des rechtlichen Umgangs mit Kundendaten überlegen müssen. Vor diesem Hintergrund wird deutlich, dass nicht nur – wie von Roßnagel angesprochen – die Informatik gefordert ist. Diese liefert bspw. mit dem P3P-Standard bereits Lösungen, die von den Unternehmen aufgegriffen werden können. Vielmehr sollten Informationssysteme unter Berücksichtigung der fachlichen Herausforderungen intelligent (weiter)entwickelt werden. Diese liegen im vorliegenden Fall in der Neuausrichtung der Beratungsprozesse aufgrund der (teilweise neuen) gesetzlichen Anforderungen. Hierbei steht im Vordergrund die Aufgabe, eine qualitativ hochwertige Beratung zu ermöglichen und dabei die Beziehung zum Kunden vertrauensvoll zu gestalten, sodass dieser die Verarbeitung seiner personenbezogenen Daten billigt, weil er für deren Preisgabe eine angemessene Gegenleistung erhält. Die im Beratungsprozess notwendigen Daten zur Verfügung zu stellen, um den Kunden ideal beraten zu können, ist die primäre Aufgabe von Informationssystemen, die Einhaltung der Datenschutzvorschriften „nur“ eine notwendige Nebenbedingung.

Vertreter der Praxis äußern neben den hohen Kosten, welche die Umstellungen aufgrund der beiden EU-Richtlinien mit sich bringen, auch Bedenken dahingehend, dass die Dokumentationspflicht zu einem Rückgang des Absatzes führen wird. Neben einer zu erwartenden höheren Beratungsqualität und damit einhergehender gesteigerter Kundenzufriedenheit bieten sich jedoch für die Unternehmen weitere Nutzenpotenziale. Zunächst lässt sich ein verbessertes Cross-Selling nennen, da Finanzdienstleister ihre Kunden aufgrund der dokumentierten Daten gezielter auf einen bestimmten Bedarf ansprechen können. Zudem müssen für die Umsetzung der Richtlinien ohnehin Projekte initiiert und der damit verbundene Aufwand geleistet werden. Die Unternehmen könnten diesen Rüstaufwand nutzen und die Zielsetzung derartiger Projekte dahingehend erweitern, dass ein Schritt in Richtung kundenzentrierter Informationssysteme erfolgt. Aber auch wenn nur die Mindestanforderungen aus den EU-Richtlinien erfüllt werden, profitieren Unternehmen mit de-

ren Umsetzung durch eine höhere Datenqualität. Diese wiederum führt – unter Berücksichtigung der datenschutzrechtlichen Vorschriften – z.B. zu höheren Erfolgsquoten im Kampagnenmanagement oder zu einer genaueren Abschätzung der Potenziale einzelner Kunden oder Kundengruppen. Finanzdienstleister sollten also nicht nur den Aufwand der regulatorischen Anforderungen sehen, sondern die dahinter stehenden Kundenbedürfnisse sowie die sich hieraus ergebenden Chancen erkennen.

Literatur

1. Arbeitskreis EU-Vermittlerrichtlinie Dokumentation (Hrsg) (2007) Hausrat Risikoanalyse. <http://www.vermittlerprotokoll.de/download/hausrat/hausratrisikoanalyse.doc> (Abruf am 2007/11/01)
2. Berendt B, Günther O, Spiekermann S (2005) Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. *Commun ACM* 48:101–106
3. Brockhausen J, Bürkin K, Renz H (2007) Bearbeitungs- und Prüfungsleitfaden MiFID: Umsetzungsanleitung und Umsetzungsprüfung für die Praxis von Banken und Sparkassen. In: Becker A et al. (Hrsg) *Internal Audit Strategy*. Bankakademie, Frankfurt am Main
4. Buhl HU, Kundisch D, Steck W (2002) Sophistication Banking als erfolgreiche Strategie im Informationszeitalter. *Z Betriebswirt* 72:1–12
5. Bund der Versicherten (2007) Hausrat – Bedarf. http://www.bunderversicherten.de/bdv/default.asp?ContentUrl=http://www.bunderversicherten.de/bdv/Versicherungsarten/Hausrat/bedarfhausrat.htm&TopUrl=/bdv/navi/headline_show.asp?headline=Bedarf (Abruf am 2007/11/01)
6. Bundesministerium für Wirtschaft und Technologie (2006) Bundeskabinett beschließt Entwurf eines Gesetzes zum Abbau bürokratischer Hemmnisse. <http://www.bmwi.de/BMWi/Navigation/Presse/pressemitteilungen,did=130126.html> (Abruf am 2007/11/01)
7. Chellapa R, Sin R (2005) Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Inf Technol Manage* 6:181–202
8. Duve C, Keller M (2006) MiFID: Die neue Welt des Wertpapiergeschäfts oder: Glauben Sie nicht, Sie könnten ohne weiteres Wertpapiere kaufen. *Betriebsberater* 61:2477–2484
9. Fiala J (2007) Nur wer gut berät, ist gut geschützt. *Versicherungsmagazin* 54: 64–65
10. Franke T (2001) P3P – Platform for Privacy Preferences Project. *Wirtschaftsinformatik* 43:197–199
11. Hailstone R (2001) memIQ erlaubt die Integration und das Management persönlicher Dokumente. *Datenbank-Spektrum* 1:53–58
12. Hamann G (2007) Meine Daten sind frei. <http://www.zeit.de/2007/45/01-Internet> (Abruf am 2007/11/01)
13. Kaas KP, Severidt K (2002) Neue Preismodelle in der Kapitalanlageberatung der Banken? *Z Betriebswirt* 72:619–640
14. Kleinz T (2007) Daten-Gau bei StudiVZ. http://www.focus.de/digital/internet/online-community_nid_45470.html (Abruf am 2007/11/01)
15. Krüger A (2007) Neuer Daten-GAU bei eBay – Millionen Nutzerdaten im Internet frei zugänglich. <http://www.heute.de/ZDFheute/inhalt/11/0,3672,7118219,00.html> (Abruf am 2007/11/01)
16. Maschmeyer C (2007) Vermittlerrichtlinie: Unabhängige als Gewinner. *Bank Markt* 36:16–18
17. Mertens P (2006) Das Ungleichgewicht im Datenschutz. *Informatik-Spektrum* 29: 416–423
18. Mertens P, Grieser J (2002) Integrierte Informationsverarbeitung. *Planungs- und Kontrollsysteme in der Industrie*, Bd. 2. 9. Aufl. Gabler, Wiesbaden
19. Opatkowski HW, Duncker C (2001) *Der gläserne Konsument – Die Zukunft von Datenschutz und Privatsphäre in einer vernetzten Welt*. BAT-Freizeit-Forschungsinstitut, Hamburg
20. Roßnagel A (2005) Verantwortung für Datenschutz. *Informatik-Spektrum* 28: 462–473
21. Roßnagel A (2007) Personalisierung in der E-Welt – aus dem Blick der informationellen Selbstbestimmung gesehen. *Wirtschaftsinformatik* 49:26–33

22. Schmidt-Gallas D, Lauszus D, Burger V (2007) Versicherungsvertrieb im Umbruch
23. Schwenke MC (2006) Individualisierung und Datenschutz – Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung. Deutscher Universitäts-Verlag, Wiesbaden
24. Stiftung Warentest (Hrsg) (2003) Schlecht beraten. Finanztest 13:12–17
25. Stiftung Warentest (Hrsg) (2006) Versicherungsvermittlung – Etwas mehr Sicherheit für Kunden. http://www.stiftung-warentest.de/online/versicherung_vorsorge/meldung/1447512/1447512.html (Abruf am 2007/11/01)
26. Stiftung Warentest (Hrsg) (2007) Beraten und verkauft. Finanztest 17:12–16
27. Tilmes R (2001) Financial Planning im Private Banking – Kundenorientierte Gestaltung einer Beratungsdienstleistung. Uhlenbruch, Bad Soden/Ts
28. Tinnefeld M, Ehmann E, Gerling R (2005) Einführung in das Datenschutzrecht – Datenschutz und Informationsfreiheit in europäischer Sicht. Oldenbourg, München Wien
29. Treiblmaier H (2007) Beziehungsmarketing aus Kundensicht. Wirtschaftsinformatik 49:42–48
30. Warth W, Beenken M (2005) Bank Markt 55:36–38
31. Yildirim N (2004) Datenschutz im Electronic Government – Risiken, Anforderungen und Gestaltungsmöglichkeiten für ein datenschutzgerechtes und rechtsverbindliches eGovernment. Deutscher Universitäts-Verlag, Wiesbaden