

# Datenschutz als Chance verstehen

Von Michael G. Möller



**Obwohl die Anforderungen an den Datenschutz durch die Novellen des Bundesdatenschutzgesetzes deutlich verschärft wurden, wird der Handlungsbedarf in der Bankenwelt noch nicht ausreichend wahrgenommen, mahnt Michael G. Möller. Angepasst werden müssen alle Prozesse einschließlich der IT-Systeme, von den operativen bis zu den vertriebsunterstützenden Systemen. Die Umsetzung der rechtlichen Vorgaben sollte aber nicht nur als notwendiges Übel verstanden werden. Vielmehr biete der aktive Umgang mit dem Thema Datenschutz auch Ansätze für eine positive Differenzierung im Wettbewerb.** Red.

Die Bedeutung des Datenschutzes im wirtschaftlichen Handeln hat in den vergangenen Jahren kontinuierlich zugenommen. Die Verbraucher sind durch die jüngsten Skandale im Zusammenhang mit Datenmissbrauch besonders sensibilisiert. Die Weiterentwicklung des Bundesdatenschutzgesetzes (BDSG) – zuletzt mit der Novelle III im Juni 2010 – trägt dieser Entwicklung auch im Bereich der direkten werblichen Kundenansprache Rechnung. Dabei ist nicht nur ein umfangreicherer Schutz des Verbrauchers im Sinne der informationellen Selbstbestimmung berücksichtigt. Vielmehr wurden darüber hinaus auch mögliche Haftungsfolgen

und potenzielle Imageschäden für das verantwortliche Management des werbenden Unternehmens konkretisiert. Dies betrifft in besonderer Weise Finanzdienstleister – gerade solche im Endkundengeschäft.

Da für Retailbanken und Sparkassen die Bedeutung von Multichannel-Aktivitäten permanent zunimmt, müssen sich verantwortliche Manager mit der Frage beschäftigen, inwieweit Vertrieb, Marketing, Governance und Organisation den jüngsten Entwicklungen Rechnung tragen – insbesondere in Bezug auf die werbliche Ansprache des Kunden. Um rechtskonformes Agieren und die Handlungsfähigkeit in Marketing und Vertrieb sicherzustellen, sind Aufbau- und Ablauforganisation in Bezug auf vorhandenes Gefährdungspotenzial hin zu untersuchen, geeignete Maßnahmen festzulegen und rasch umzusetzen.

Wesentlich sind die Voraussetzungen für die Erhebung, Speicherung und Verwendung von Daten für die werbliche Ansprache des Kunden, mithin das Dialogmarketing zwischen werbungtreibenden Unter-

nehmen und Verbrauchern. Für Letzteres existieren strenge Richtlinien, deren Missachtung gemäß § 43 BDSG mit Geldbußen von bis zu 300 000 Euro und in einigen Fällen noch höher geahndet werden kann. Für die werbliche Adressnutzung existieren folgende Voraussetzungen:

- Der Betroffene muss bei der Datenerhebung die Information erhalten, wer für welche Zwecke seine personenbezogenen Daten nutzt.
- Die aktive/ausdrückliche (schriftliche) Zustimmung (Opt-in) des Betroffenen muss für diejenigen Telekommunikationskanäle vorliegen, die das werbungtreibende Unternehmen im Kundendialog mit dem einzelnen Kunden einsetzen möchte. Die schriftliche Bestätigung muss vorliegen für E-Mail-Werbung, Telefonmarketing, Faxwerbung oder SMS/MMS-Werbung.
- Dem Auskunftsanspruch des Betroffenen kann entsprochen werden; das heißt ein Kunde kann vom werbungtreibenden Unternehmen zum Beispiel die Information verlangen, auf welcher rechtlichen Basis ein Werbekontakt erfolgt ist.

## Zum Autor

**Michael G. Möller** ist Managing Partner von KWF Business Consultants GmbH, Frankfurt am Main.

Die größten Änderungen gegenüber der bisherigen Rechtslage gibt es bei der Verwendung von Daten zu Werbezwecken (§ 28 Abs. 3 BDSG). Die Nutzung ist demnach in den meisten Fällen nur noch mit Einwilligung des Betroffenen zulässig

(Opt-in). Zwar ist es durch das Listenprivileg weiterhin möglich, Daten für bestimmte Zwecke auch ohne Opt-in zu nutzen oder zu verarbeiten. Aber auch hierbei sind juristische Auflagen streng zu beachten. Unter anderem muss aus der Werbung hervorgehen, wer die personenbezogenen Daten eines Betroffenen als erstes Glied in der Nutzungskette erhoben hat. Auf Anfrage eines Betroffenen sind dieser Nachweis und die Erlaubnis, wozu die Daten genutzt werden dürfen, vom werbungstreibenden Unternehmen zu erbringen. Letzteres bedeutet hohen organisatorischen, prozessualen und technischen Aufwand.

**Alle Prozesse anpassen**

Um die vom Betroffenen erlaubten Kommunikationswege nutzen zu dürfen, bedarf es der expliziten Zustimmung jedes einzelnen Kunden oder Interessenten. Um einen Kunden beispielsweise telefonisch (ebenso E-Mail, Fax, SMS, MMS) kontaktieren zu dürfen, muss dieser vorher möglichst schriftlich zugestimmt haben. Zwar gilt auch die mündliche Zustimmung, aber in Kombination mit einem eventuell mehrere Jahre nach erteilter Erlaubnis zu erbringenden Nachweis fällt dies bei Vorlage eines Schriftstücks sicher am leichtesten.

Für Unternehmen, die mit ihren Kunden und Interessenten über verschiedene Kommunikationswege in Kontakt treten wollen, bedeutet dies in der Folge die Anpassung aller Prozesse zu den Themen Erfassung, Speicherung und Verwendung von personenbezogenen Daten.

**Informationspflichten bei Datenpannen**

Bezüglich der gesteigerten Informationspflichten ist dem US-amerikanischen Vorbild folgend nun festgelegt, dass bei unrechtmäßiger Kenntniserlangung von Dritten schon bei drohendem Datenmiss-

brauch eine Mitteilung an die zuständige Datenschutzbehörde abzugeben ist (§ 42a BDSG). Stellt die verantwortliche Stelle daraufhin fest, dass den Betroffenen „schwerwiegende Beeinträchtigungen“ drohen, sind diese sowie auch die Aufsichtsbehörden durch das Unternehmen zu informieren. Erfordert die Benachrichtigung der Betroffenen, zum Beispiel wegen der Vielzahl der Fälle, einen unverhältnismäßig großen Aufwand oder zu viel Zeit, ist die Öffentlichkeit alternativ durch Anzeigen (mindestens eine halbe Seite) in zwei deutschlandweit erscheinenden Tageszeitungen zu informieren.

Es wird rasch deutlich, dass die genannten Voraussetzungen erhebliche Implikationen auf die Geschäftsprozesse und IT-Systeme der Finanzdienstleister haben. Denn dies bedeutet in der Praxis, dass die entsprechenden Informationen je Kunde erhoben, gespeichert und jederzeit abrufbar sein müssen – und zwar für jeden Werbe- und Kontaktkanal einzeln.

Durch die jüngsten Novellen des BDSG haben sich Anforderungen an und potenzielle Risiken für die Unternehmen dramatisch erhöht. Innerhalb der Bankenwelt ist der Handlungsbedarf bisher jedoch noch nicht hinreichend wahrgenommen

worden. So sind organisatorische Verantwortlichkeiten häufig unklar oder unvollständig geregelt. Datenschutzblätter und Einwilligungserklärungen tragen der aktuellen Rechtslage nicht hinreichend Rechnung und ein systematischer Prozess zur Erhebung und Pflege der kundenbezogenen Daten existiert nicht – so lautet in vielen Fällen das Fazit in deutschen Banken.

**Operative und CRM-Systeme einbeziehen**

Die gesetzlichen Anforderungen machen es erforderlich, Opt-in- und Opt-out-Informationen systematisch zu erfassen, wobei praktisch immer sowohl operative Kundensysteme als auch Vertriebsunterstützungs- beziehungsweise CRM-Systeme einzubeziehen sind. Es geht praktisch nicht ohne die Einbeziehung der IT-Systeme – diese stellen allerdings auch nicht die Lösung dar.

Das Management muss zunächst Klarheit über die Gefährdungssituation erlangen und Entscheidungen über Planung und Umsetzung entsprechender Maßnahmen zum Thema „Umgang mit personenbezogenen Daten“ mit folgendem Schwerpunkt treffen:

**Abbildung 1: Datenschutz und Datensicherheit als Teil der Unternehmensstrategie**

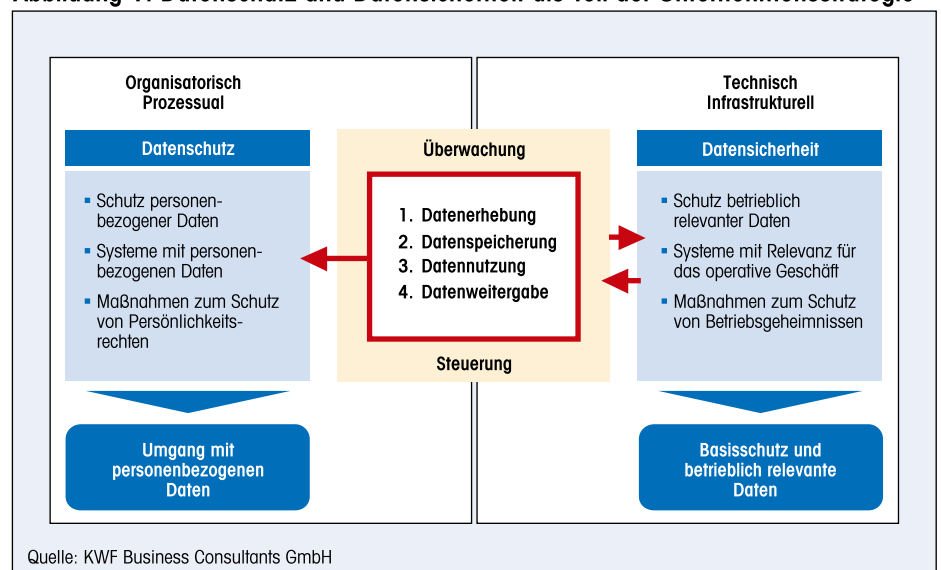
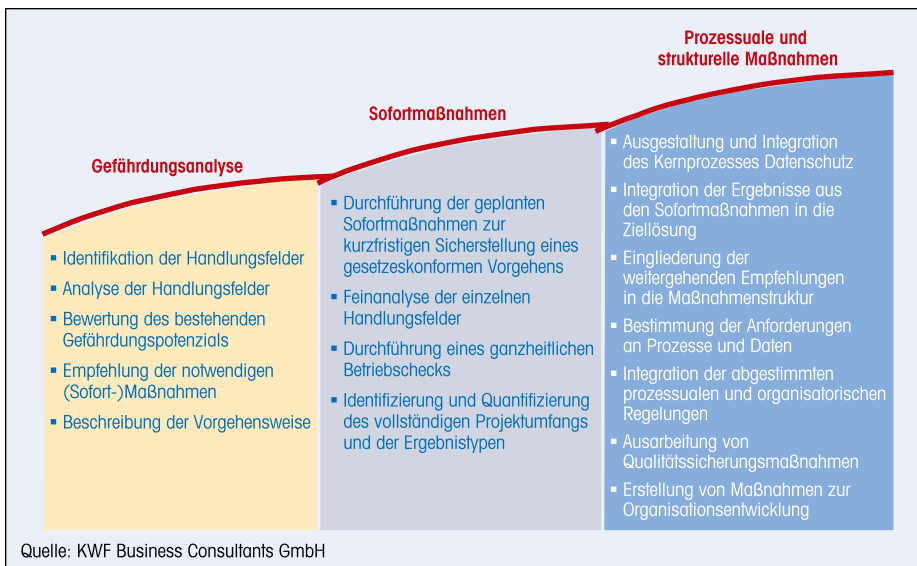


Abbildung 2: Vorgehensmodell zum Umgang mit personenbezogenen Daten



■ Transparenz über relevante Aspekte und deren Risikopotenzial;

■ strategische Positionierung der Bank zum Umgang mit personenbezogenen Daten;

■ Definition von Maßnahmen zur aktiven Risikosteuerung und zur nachhaltigen Erfüllung rechtlicher Anforderungen im Umgang mit personenbezogenen Daten;

■ Beschreibung und Umsetzung priorisierter Sofortmaßnahmen zur Einhaltung datenschutzrelevanter Bestimmungen, sofern notwendig;

■ Beschreibung notwendiger Projektaktivitäten für die Umsetzung struktureller Maßnahmen in den Themenfeldern Governance, Organisation und IT.

Damit eine signifikante Einschränkung und schlimmstenfalls dauerhafte Blockade der Vertriebsaktivitäten vermieden wird, hat sich ein mehrstufiges Vorgehensmodell entlang der Unternehmensprozesse bewährt. Hier setzen sinnvollerweise auch Organisationsentwicklungsmaßnahmen an, um dem Vertrieb die „Angst vor Handlungsunfähigkeit“ zu nehmen. Ein Gefährdungs-Check kann dem Management helfen, mit Hilfe strukturierter Fragelisten

unternehmensspezifische Handlungsfelder im Unternehmen vollständig und schnell zu identifizieren.

Sollten im Rahmen dieser Analyse Gefährdungspotenziale sichtbar werden, können mit Hilfe von Checklisten zügig die notwendigen Sofortmaßnahmen entwickelt und eingeleitet werden. Das Risiko, gegen datenschutzrechtliche Vorgaben zu verstoßen, lässt sich damit in kurzer Zeit erheblich reduzieren.

### Vorgehensmodell zum Umgang mit personenbezogenen Daten

Sollte die Analyse ergeben, dass außer der Durchführung der genannten Sofortmaßnahmen zur schnellen Sicherstellung gesetzeskonformen Handelns weiterer Handlungsbedarf in Bezug auf die Erhebung, Speicherung, Nutzung oder Weitergabe von Daten besteht, ist eine anschließende Feinanalyse der betroffenen Prozesse sinnvoll. Mit den Ergebnissen dieser Untersuchung ist es dann möglich, zu identifizieren und zu quantifizieren, welche organisatorischen und IT-bezogenen Maßnahmen nötig sind, um Risiken weiter zu reduzieren und die dauerhafte Handlungsfähigkeit des Unternehmens sicherzustellen.

Nach zirka sechs bis acht Wochen sollten folgende wesentlichen Schritte erledigt sein:

■ klar definiert, wann eine Datenschutzpanne vorliegt, die eine Meldung an die zuständige Aufsichtsbehörde erforderlich macht,

■ Meldeprozesse und Vorgehensweise bei der Information der Betroffenen festgelegt,

■ Schwachstellen (zum Beispiel bei der Verschlüsselung von Daten) analysiert und adäquate Gegenmaßnahmen ermittelt,

■ datenschutzrelevante Prozesse im Unternehmen identifiziert,

■ Auskunftsprozesse nach automatisierten Einzelentscheidungen analysiert,

■ sichergestellt, dass Datenschutzblätter und Einwilligungserklärungen rechtskonform und vollständig im Sinne der Unternehmenspositionierung sind,

■ kontrolliert, ob die Zustimmung der Kunden zur Werbeansprache für alle strategisch definierten Telekommunikationswege – Stichwort Multi-Channel-Vertrieb – vorliegt und gegebenenfalls Maßnahmen zu Einholung angestoßen,

■ sichergestellt, dass Kunden und Interessenten nur über die von ihnen persönlich erlaubten Kommunikationskanäle angesprochen werden,

■ sichergestellt, dass bei der Nutzung übermittelter Daten immer die Nennung der erhebenden Stelle erfolgt, und

■ Potenziale aufgezeigt, welche Möglichkeiten zur Nutzung personenbezogener Daten im Rahmen regulatorischer Anforderungen bestehen.

Nach Abschluss der notwendigen Sofortmaßnahmen ist zu entscheiden, in welchem Umfang Datenschutz und der damit

verbundene Umgang mit personenbezogenen Daten in die bestehenden Geschäfts- und Unternehmensprozesse sowie die IT-Systeme zu integrieren ist. Dazu sollten neben der Bestimmung der Anforderungen an die Prozesse und der Integration der prozessualen und organisatorischen Regelungen begleitend auch Maßnahmen und Strukturen zur Qualitätssicherung einbezogen werden. Damit ist der Grundstein gelegt für ein integriertes Datenschutz- und -sicherheitsmodell, das für eine dauerhafte Verankerung im Unternehmen unverzichtbar geworden ist.

Als Fazit lässt sich festhalten: Der Datenschutz hat in den vergangenen Jahren zunehmende Bedeutung erlangt und wird

doch in der Regel als „notwendiges Übel“ wahrgenommen. Heute reicht es für Finanzdienstleister jedoch nicht mehr aus, allein gesetzlichen Anforderungen gerecht zu werden und die Beschränkungen der Handlungsfähigkeit gerade im Vertrieb zu beklagen.

### Datenschutz als Differenzierungsmerkmal

Der aktive Umgang mit dem Recht des Verbrauchers auf informationelle Selbstbestimmung kann ganz im Gegenteil dazu dienen, Alleinstellungsmerkmale im Markt zu generieren und gegenüber dem Kunden echten Mehrwert zu erzeugen. Es

bietet sich die Chance, höhere Sicherheitsstandards aktiv gegenüber dem Kunden zu vermarkten und damit Glaubwürdigkeit zu erhöhen und Vertrauen zu stärken – dem wesentlichen Asset in der Kundenbeziehung bei Banken. Nach innen gerichtet kann das Thema als Enabler genutzt werden, um Kundenorientierung stärker zu leben und den Kundendialog in bedarfsgerechter Weise zu intensivieren.

Hierfür sollte sich das Management rasch in einem ersten Schritt Überblick über mögliche Gefährdungspotenziale und Risiken verschaffen – handelt es sich doch hierbei nicht zuletzt um das Risiko der persönlichen Haftung. ■

## „Konkret messbarer Nutzen“

**Herr Möller, immer wieder geraten Banken und Sparkassen wegen Verstößen gegen den Datenschutz in die Schlagzeilen. Auch Institute aus der ersten Reihe scheinen das Problem trotz großer IT- und Rechtsabteilungen nicht in den Griff zu bekommen. Woran liegt das aus Ihrer Sicht?**

**Möller:** Datenschutz und insbesondere der Umgang mit personenbezogenen Daten werden in vielen Häusern immer noch als Zusatzaufgabe, ja manchmal sogar als ein notwendiges Übel betrachtet, das bei den von Ihnen genannten Abteilungen abgeladen wird. Eine Bank, die so denkt, kann aber so viele Fachleute mit technischem und juristischem Sachverstand einstellen wie sie will, ohne das Risiko einer Datenpanne dadurch wirklich zu reduzieren.

**Wie können die Kreditinstitute hier Abhilfe schaffen?**

**Möller:** Der Umgang mit personenbezogenen Daten ist ein klassisches Querschnittsthema, das über alle Organisationseinheiten hinweg gemanagt werden

muss. An erster Stelle steht die grundlegende Bereitschaft, dies als wesentliche Unternehmensaufgabe zu akzeptieren. Mitarbeiter sind zu sensibilisieren, Prozesse beziehungsweise Technik sind auf relevante Aspekte hin zu untersuchen und anzupassen. Ein Patentrezept gibt es dabei nicht, da die jeweiligen Maßnahmen sehr stark vom einzelnen Unternehmen abhängen. Wichtig ist jedoch, dass eindeutige Verantwortlichkeiten bestimmt sind. Bei großen Unternehmen durch eine übergreifende Sicherheitsorganisation, bei kleineren Unternehmen durch einen Gesamtverantwortlichen im Vorstand oder in der Geschäftsleitung. Alles andere würde das falsche Signal an die Mitarbeiter aussenden.

**Apropos Mitarbeiter. Wie kann die Belegschaft über das Vorbild durch die Führungskräfte hinaus noch motiviert werden, den Umgang mit personenbezogenen Daten wirklich ernst zu nehmen?**

**Möller:** Indem jedem Mitarbeiter der Zusammenhang zwischen Datenschutz, Kundenorientierung und damit letztendlich

geschäftlichem und persönlichem Erfolg erklärt wird. Eine Bank, die mit einem über die gesetzlichen Vorgaben hinausgehenden Datenschutz echten Mehrwert für ihre Kunden erzeugt, kann den Kundendialog nämlich auf eine ganz andere Basis stellen. Und diese Intensivierung schlägt sich eben nicht nur in weichen Faktoren nieder, sondern führt auch zu geringeren Prozesskosten bei Vertrieb und Abwicklung, verbesserten Cross-Selling-Quoten und niedrigeren Abwanderungsraten – also zu konkret messbarem Nutzen.



*Michael G. Möller ist seit Sommer 2008 Managing Partner der KWF Business Consultants GmbH in Frankfurt am Main. Zuvor hatte er verschiedene Führungsfunktionen bei namhaften Unternehmensberatungen und in der Industrie inne. Der studierte Wirtschaftsingenieur verfügt über mehr als 20 Jahre Erfahrung aus zahlreichen Beratungsmandaten und (Groß-)Projektleitungen bei Industrie- und (Finanz-)Dienstleistungsunternehmen in ganz Europa.*