

# Herausforderung Datenschutz

Neuer Umgang der IT mit personenbezogenen Daten

Die Weiterentwicklung des Bundesdatenschutzgesetzes (BDSG) – zuletzt mit der Novelle III im Juni 2010 – hat auf die Unternehmen der Finanzdienstleistungsbranche erhebliche Auswirkungen. Da die Institute der Branche in der Regel viele sensible Kundendaten entlang der gesamten Prozesskette verarbeiten, muss die Unternehmens-IT in der Lage sein, diese Prozesse technisch zu unterstützen und abzusichern. Weil die Anforderungen an einen leistungsfähigen Datenschutz stetig wachsen, verstärkt sich der Handlungsdruck sogar noch.

Kunden werden für Finanzdienstleister künftig verstärkt über interaktive Plattformen wie Facebook und Twitter erreichbar sein. Diese stellen zusätzliche Anforderungen an den Umgang mit personenbezogenen Daten. Eine Ruhepause können sich die Unternehmen daher keinesfalls leisten. Verstöße gegen das BDSG werden zudem mit empfindlichen Strafen geahndet. Deutlich schwerer wiegt allerdings der Imageschaden nach Bekanntwerden einer Datenpanne. Denn mangelnde Sorgfalt beim Umgang mit persönlichen Kundendaten und die damit verbundene Verletzung von Persönlichkeitsrechten kann das Kundenvertrauen – das Fundament jeder Geschäftsbeziehung – nachhaltig erschüttern. Dies gilt umso mehr, als die Öffentlichkeitswirkung von Verstößen groß ist. Zu den personenbezogenen Daten gehören nach §3 Abs. 1 des BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person“. Für die Erhebung, Verarbeitung, Nutzung, Übermittlung und Überwachung derartiger Daten muss es im Unternehmen Strukturen geben, die den gesetzeskonformen Umgang mit diesen Daten nachweisbar sicherstellen. Dabei gilt der Grundsatz: Eine Verwendung von personenbezogenen Daten darf nicht ohne Rechtsvorschrift oder Genehmigung des Betroffenen erfolgen – etwa in Form einer Einwilligungserklärung (EWE). Die Verantwortung für die Einhaltung geltender Gesetze trägt der Vorstand beziehungsweise die Geschäftsführung des Finanzdienstleisters. Die operative Verantwortung liegt beim Datenschutzbeauftragten, der die Erfüllung der Anforderungen aus dem Datenschutzgesetz in den Fachabteilungen und dem IT-Bereich zu überwachen hat.

## Datenschutz erstreckt sich über die gesamte IT-Architektur

Die größte Herausforderung für Finanzdienstleister besteht darin, dass die Datenschutz-Anforderungen nicht mehr auf einzelne,

isolierte IT-Systeme beschränkt sind. Sie wirken inzwischen im Querschnitt auf die gesamte IT-Architektur. Grund hierfür ist ein Paradigmenwechsel im Selbstverständnis des Datenschutzes. Früher standen hier vertragsbezogene Funktionalitäten im Fokus, heute wird das Individuum selbst, mitsamt seiner persönlichen Daten, als schützenswert eingestuft. Nun geht es verstärkt darum, datenschutzrelevante Anforderungen wie Nachvollziehbarkeit von Datenzugriffen, Berücksichtigung des personenbezogenen Datenschutzprofils und aktive Steuerung von Datenschutzrisiken in die Applikationslandschaft des Unternehmens zu integrieren. Für das IT-Management hat dies zur Folge, dass die IT-Landschaft grundsätzlich sowie in den unterschiedlichen Geschäfts-

### Checkliste für Ihren IT-Bereich: Wie groß ist Ihr Handlungsbedarf im Umgang personenbezogener Daten

- Besteht Transparenz darüber, in welchen Systemen personenbezogene Daten gespeichert, verarbeitet und genutzt werden?
- Sind diese Systeme entsprechend abgesichert und gegen Missbrauch geschützt?
- Liegen notwendige Freigaben der Betroffenen zur Verarbeitung und Verwendung der personenbezogenen Daten vor?
- Werden diese Daten gemäß BDSG zweckgebunden verarbeitet?
- Werden bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten die Vorschriften zur Datenvermeidung und Datensparsamkeit eingehalten und gibt es im Unternehmen hierzu verbindliche Festlegungen?
- Werden personenbezogenen Daten auf Wunsch der Betroffenen in IT-Systemen gelöscht?
- Werden die Vorschriften zur Übermittlung von personenbezogenen Daten an Dritte und ggf. ins Ausland eingehalten („Auftragsdatenverarbeitung“)?
- Wurden hinreichende Maßnahmen zur Kontrolle der Einhaltung des BDSG getroffen?
- Werden Verstöße beim Umgang mit personenbezogenen Daten unverzüglich an den Datenschutzbeauftragten gemeldet?
- Wird der Datenschutzbeauftragte in IT-Projekte, die den Umgang mit personenbezogenen Daten betreffen, einbezogen?

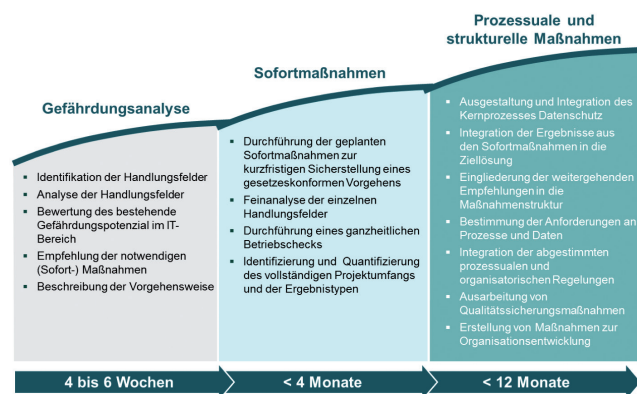
applikationen entsprechend zu überprüfen ist und den aktuellen Anforderungen gegenübergestellt wird. Das Zusammenspiel der einzelnen betriebswirtschaftlichen Applikationen muss gegebenenfalls neu aufeinander abgestimmt werden. Die damit verbundenen operativen Prozesse sind daher, in enger Zusammenarbeit mit dem Fachbereich, an den notwendigen Stellen anzupassen. Dabei ist zu beachten, dass eine Einwilligungserklärung zur Verwendung der Daten immer personenbezogen ist. Aus IT-Sicht kann dies vor allem dann zu Problemen führen, sobald mehrere Personen beziehungsweise Benutzerrollen in einem Vertrag zu berücksichtigen sind. In diesem Fall sind mehrere Einwilligungserklärungen für diesen Vertrag im System zu hinterlegen. Doch in vielen Fällen sind das Datenmodell und die Schnittstellen zwischen den Applikationen dafür nicht ausgelegt – die IT müsste entsprechend der neuen Anforderung angepasst werden.

### Vorsicht bei Kundendaten für Vertriebs- und Werbezwecke

Weitere Probleme mit der Einwilligungserklärung können vor allem dann auftreten, wenn Kundendaten für Vertriebs- und Werbezwecke genutzt werden sollen. Bei jeder Selektion in der Kundendatenbank ist nun zu prüfen, ob eine gültige Einwilligungserklärung zur werblichen Ansprache vorliegt. Nur diejenigen Kunden dürfen per E-Mail, Telefon oder über soziale Netzwerke angesprochen werden, die ihre Zustimmung gegeben haben. Zusätzlich müssen Strukturen bestehen, die es ermöglichen, dass von Kunden unterschriebene EWE-Dokumente über ein entsprechendes Dokumentenmanagementsystem abgerufen werden können – nur so lässt sich die Kundeneinwilligung zur Werbeanzeige bei Bedarf nachweisen. Die Regelungen im Datenschutz betreffen auch die durch die IT-Abteilung beauftragten externen Auftragsdatenverarbeiter (gemäß §11 BDSG). Auch diese sind zur Einhaltung der Anforderungen aus dem BDSG verpflichtet. Daher muss in der vertraglichen Vereinbarung der Dienstleister zumindest auf die Einhaltung des im BDSG genannten „Zehn-Punkte-Katalogs“ schriftlich verpflichtet werden. Hiervon betroffen sind auch rechtlich eigenständige IT-Bereiche in einem Konzernunternehmen.

Damit der Umgang mit personenbezogenen Daten langfristig auf einer soliden Basis steht, müssen die Anforderungen aus dem BDSG in vorhandenen Datenmodellen abgebildet und die Einwilligungserklärungen technisch integriert werden. Die Verwendung der Daten muss im Funktionsmodell festgeschrieben sein und nachvollziehbar dokumentiert werden. Wesentlich ist dabei die saubere Integration der BDSG-Anforderungen in die operativen Abläufe, um die Geschäftsprozesse nicht übermäßig zu verkomplizieren und das operative Geschäft nicht zu behindern. Um sich im IT-Bereich der Gesamtaufgabe strukturiert zu stellen, hat sich ein dreistufiges Vorgehen bewährt (Siehe Abbildung 1 „Dreistufiges Vorgehensmodell zur Umsetzung der Anforderungen aus dem BDSG“):

Bei der Anwendung dieses Vorgehensmodells lässt sich der Handlungsbedarf beim Umgang mit personenbezogenen Daten schnell herausarbeiten. In drei Schritten lassen sich die Ergebnisse zügig in ein unternehmensweites Sicherheitskonzept überführen. Eine Gefährdungsanalyse soll zunächst sicherstellen, dass



Dreistufiges Vorgehensmodell zur Umsetzung der Anforderungen aus dem BDSG

die größten Datenschutzrisiken im Unternehmen identifiziert werden. Diese gilt es über Sofortmaßnahmen zu beseitigen, um gesetzeskonformes Arbeiten zu gewährleisten. Da vier von zehn Unternehmen in der Regel gleich mehrmals von Datenpannen betroffen sind, ist bei der anschließenden Planung und Umsetzung von strukturellen Maßnahmen große Sorgfalt erforderlich. Das Denken in durchgängigen Prozessen ist dabei die wesentliche Grundlage für alle Aktivitäten.

### Fazit

Der rechtskonforme Umgang mit personenbezogenen Daten ist häufig eine große Herausforderung für Finanzdienstleister. Schon ein einzelner Verstoß gegen die einschlägigen Normen kann erhebliche negative Folgen für das Unternehmen haben. Daher sollte der richtige Umgang mit Kundendaten ein fester Bestandteil der Unternehmens- und IT-Strategie sein. Situative Einzelanpassungen sind hierbei keine nachhaltige Lösung. Nur über einen Gesamtlösungsansatz sind Unternehmen in der Lage, die Verwendung von personenbezogenen Daten ohne Erhöhung der Prozesskosten und Störung der Geschäftsprozesse aufzusetzen. Die IT spielt hierbei eine tragende Rolle. Datenschutz nur organisatorisch abzubilden führt nicht zu tragfähigen und nachhaltigen rechtskonformen Lösungen. Der Gesetzgeber fordert technisch durchgängige Prozesse und Funktionen mit hinreichender vorausschauender Missbrauchsvermeidung, transparenter, dokumentierter Nutzung und weitreichender Selbstbestimmung durch die betroffenen Personen. Im Zielkonflikt zwischen gesetzlichen Anforderungen und der zwingend erforderlichen Nutzung personenbezogener Daten in den Geschäfts- und vor allem Vertriebsprozessen ist die IT gefordert, aktiv Lösungen mitzugestalten, um die zunehmenden Anforderungen des Datenschutzes nicht zur strategischen Geschäftsverhinderung mutieren zu lassen.



Autor:  
**Norbert Hilger,**  
KWF Business Consultants