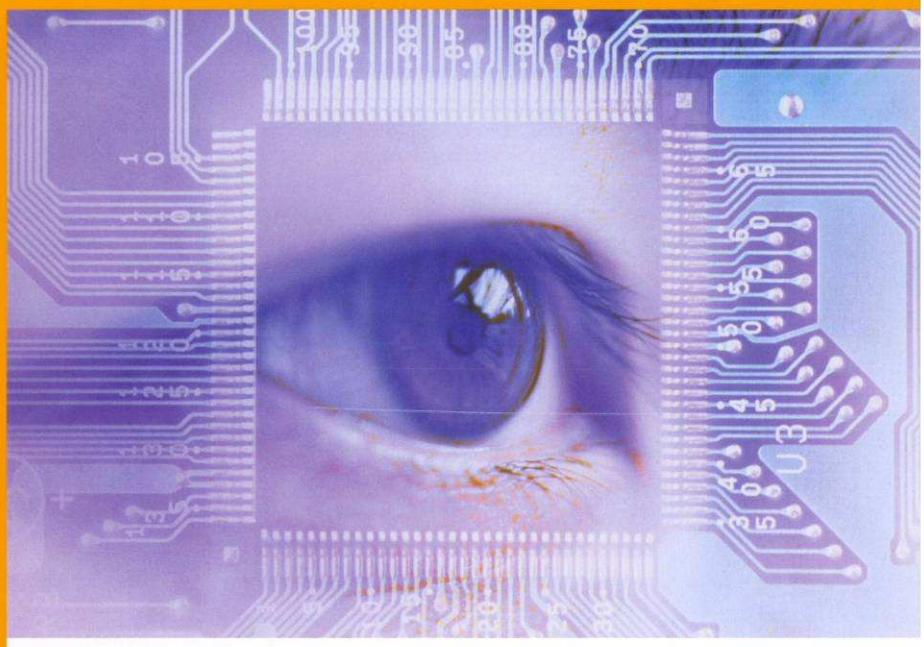
9,50 € ISSN 0042-4358 E 6945

Versicherungswirtschaft

65. Jahrgang
15. März 2010



Schwerpunkt: Elektronische Versicherungswelt

Verlag Versicherungswirtschaft

6

Datenschutz: Wie sag ich's dem Dienstleister?

Versicherer entdecken die Risiken der Neuerungen im Bundesdatenschutzgesetz und stellen Dienstleister vor materielle und organisatorische Herausforderungen. Um den Aufwand in Grenzen zu halten, müssen Versicherer und Dienstleister an einem Strang ziehen.

Thomas Fenstermacher, Karsten Kinast

Das Schreckensszenario von ein paar Säcken mit sensiblen Kundendaten in irgendeinem öffentlichen Abfallcontainer ist allgegenwärtig. Was sind die möglichen Folgen? Kundendaten werden prompt gefunden; Sicherstellung durch Polizei; Ermittlung wegen nicht sachgerechter Entsorgung sensibler Daten; Einschaltung des Datenschutzbeauftragten des Landes und des Bundes; Einschaltung der Staatsanwaltschaft; angedrohtes Bußgeld bis in die Millionen Euro. Am schlimmsten ist aber die umfangreiche und reißerische Berichterstattung in der Presse. Bei dem berechtigten Ansinnen, diesen Kelch mit dem damit verbundenen Imageschaden an sich vorbeigehen zu lassen, sind die Datenschützer der großen Versicherer nun bei deren Dienstleistern gelandet und haben dort erhebliche Sorgenfalten verursacht.

So gilt es zwar allgemein als unbestritten, das der Einsatz von Dienstleistern in der Schadenregulierung sinnvoll ist, um Kosten zu sparen. Auf der anderen Seite verlassen dabei Kundendaten aus dem sensiblen Schadenbereich das Haus – nicht ohne Risiko, dass diese an falscher Stelle wieder auftauchen.

Somit bestand und besteht hier für alle Beteiligten – Versicherer wie Dienstleister – schneller Handlungsbedarf. Der gesetzliche Anspruch ist klar definiert. Ein Dienstleister muss alle Anforderungen, die das Bundesdatenschutzgesetz (BDSG) stellt, erfüllen, und der Versicherer muss ihn dazu anhalten und kontrollieren. Hierzu gehört insbesondere der Abschluss eines Vertrages über die Auftragsdatenverarbeitung (siehe unten), der nicht nur den konkreten Auftrag beschreibt, sondern insbesondere auch die Datenschutz- und Datensicherheitsmaßnahmen des Auftragnehmers in einem Sicherheitskonzept festlegt. Vor Aufnahme der Tätigkeit muss sich der Versicherer vergewissern, dass sein Dienstleister die vereinbarten Datenschutz- und Datensicherheitsmaßnahmen erfüllen kann, also ob etwa Zugangs- und Zugriffskontrolle auf die Daten der Kunden gewährleistet sind.

Diese Anforderungen bedeuten für alle Versicherer zukünftig den notwendigen Abschied von punktuellen und unkoordinierten Maßnahmen im Bereich Datenschutz hin zu einer kompletten Neu- bzw. Erstentwicklung einer umfassenden Risikostrategie für die Abteilung Schaden/Dienstleistermanagement in Zusammenarbeit mit ihren Dienstleistern. Am Ende dieses Weges muss dann ein rechtssicherer, aber dennoch praktikabler Kooperationsvertrag stehen, dessen Anforderungen der Dienstleister auch erfüllen kann. Es ist jedoch zu befürchten, dass so mancher „Einzelkämpfer" dem Druck der hohen Kostenbelastungen bei vollumfänglicher Beachtung der Vorschriften und der kundenspezifischen Anforderungen nicht standhalten können. Derzeit sind wohl nur vereinzelt Unternehmen in der Lage, die Anforderungen vollständig zu erfüllen.

Dabei ist die Erfüllung dieser Voraussetzungen unbedingt erforderlich – eine Nichteinhaltung kann zu Verfügungen der Aufsichtsbehörden führen, etwa einer behördlichen Beendigung des Auftragsverhältnisses oder die Verhängung von Bußgeldern. Da es auf der anderen Seite jedoch im derzeitigen Marktumfeld auch nicht möglich ist, die entstehenden Kosten durch Preiserhöhungen abzufangen, bleibt zu hoffen, dass nicht zu viele kleine und gute Nischenanbieter vom „Datenschutztsuna-

Der Versicherer ist Auftraggeber einer Auftragsdatenverarbeitung gem. § 11 BDSG, der Dienstleister ist Auftragnehmer. Was bedeutet das?

- **Es ist unzureichend, auf die Verlässlichkeit des Dienstleisters ohne Weiteres zu vertrauen.**
  Auch wenn der Hauptauftrag mündlich geschlossen wird, muss eine zusätzliche, schriftliche Vereinbarung für den Bereich Datenschutz (Vertrag zur Verarbeitung personenbezogener Daten im Auftrag gem. § 11 BDSG) vorliegen.
- **Es ist unzureichend, wenn der Dienstleister lediglich erklärt, er werde das Datenschutzrecht beachten.**
  § 11 Abs. 2 BDSG enthält einen Katalog von 10 Punkten, die in einer schriftlichen Vereinbarung zur Auftragsdatenvereinbarung enthalten sein müssen:
  1. Der *Gegenstand* und die *Dauer* des Auftrags,
  2. der *Umfang*, die *Art* und der *Zweck* der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
  3. die nach § 9 zu treffenden *technischen und organisatorischen Maßnahmen*,
  4. die *Berichtigung, Löschung und Sperrung von Daten*,
  5. die nach Absatz 4 bestehenden *Pflichten des Auftragnehmers, insbesondere* die von ihm vorzunehmenden *Kontrollen*,
  6. die etwaige *Berechtigung* zur Begründung von *Unterauftragsverhältnissen*,
  7. die *Kontrollrechte* des Auftraggebers und die entsprechenden *Duldungs- und Mitwirkungspflichten* des Auftragnehmers,
  8. *mitzuteilende Verstöße* des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
  9. der Umfang der *Weisungsbefugnisse*, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
  10. die *Rückgabe* überlassener Datenträger und die *Löschung* beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.
- **Die Zeichnung einer Standardvereinbarung reicht nicht aus.**
  Der Gesetzgeber sieht eine gesonderte Vereinbarung für jeden Auftrag vor.
- **Mit einer Vereinbarung über die Auftragsdatenvereinbarung sind nicht alle gesetzlichen Anforderungen erfüllt.**
  Der Auftraggeber ist zusätzlich dazu verpflichtet, sich davon zu überzeugen, dass der Auftragnehmer die datenschutzrechtlichen Vorgaben erfüllen wird.
- **Eine Überprüfung aller Verträge gem. § 11 BDSG, die vor dem 1. 9. 2009 geschlossen wurden, ist erforderlich.**
  Hintergrund ist die an diesem Tag in Kraft getretene Datenschutznovelle, die die Anforderungen an die Verträge zur Auftragsdatenverarbeitung deutlich erhöht hat.

Stellen Sie Ihre Prozesse auf diese Anforderungen ein und profitieren Sie davon!
Nutzen Sie als Versicherer die datenschutzrechtliche Zuverlässigkeit als Herausstellungsmerkmal und werben Sie damit. Mit steigender Sensibilität wird es sich auszahlen, Datenschutz richtig zu betreiben. Imageschäden durch unsaubere Datenschutzhandhabungen können Sie vermeiden.

mi" überrollt werden. Je früher man mit der Umsetzung im eigenen Haus beginnt, umso größer ist die Chance, sich erhebliche Wettbewerbsvorteile zu verschaffen.

Es ist Sache der Versicherer, zusammen mit den Datenschutzbeauftragten rechtskonforme Prozesse zu entwickeln und diese den Dienstleistern zu vermitteln. Was muss man tun? Zunächst muss der Inhaber/die Geschäftsführung ein generelles Problembewusstsein aufbauen. Es handelt sich hier eben nicht um eine vorübergehende Modeerscheinung, die leider mit mitunter hohem finanziellen Aufwand verbunden ist, sondern um die Pflicht, datenschutzkonforme Strukturen zu schaffen. Hierzu gehört die Implementierung flexibler IT-Systeme und Prozesse, die ständig veränderte Kundenanforderungen abbilden können. Weiterhin intensive Schulung aller Mitarbeiter unter Einschaltung externer Berater und Datenschutzbeauftragten zur Sensibilisierung sowie eine schriftliche Verpflichtung auf die Einhaltung des Datenschutzes. Diese Prozesse müssen jederzeit up-to-date gehalten, allen Mitarbeitern entgegengebracht und auf neue Produkte umgestellt werden.

Beispiel: Ein Schadenregulierer, egal ob extern oder beim Versicherer angestellt, muss tagsüber sein Schlafzimmer abschließen, falls er dort einen Schreibtisch mit PC stehen hat und seine Berichte dort schreibt. Natürlich mit einbruchhemmendem Zylinderschloss. Zum Bettenmachen oder umziehen muss dieses immer auf- und unmittelbar beim Verlassen wieder abgeschlossen werden. Das gilt natürlich für alle Räume, in denen Versichererdaten vorhanden sind. Ob das jeder macht?

Notwendige Umrüstungsmaßnahmen zur datenschutzkonformen Aufstellung verursachten bei einer Schadenregulierungsorganisation mit 120 Mitarbeitern schnell hohe Einführungskosten und weiterhin natürlich laufende Belastungen zur rahmenvertragsgemäßen Erhaltung des Standards.

Die Anforderungen an den Datenschutz und damit auch die Pflicht zum ständigen Verschluss der Bürotüren gilt selbstverständlich ebenso für alle Mitarbeiter in den Versicherungsunternehmen selbst. Ein Schadenleiter, der sein Büro wieder aufschließen musste, nachdem er seine Besucher am Empfang abgeholt hat, dürfte als vorbildlich, aber auch seltene Spezies gelten.

Man kann über den Sinn und Unsinn solcher und anderer Anforderungen des BDSG streiten. Grundsätzlich handelt es sich beim Schutz der Kundendaten natürlich aber um eine sinnvolle und unumgängliche Notwendigkeit. Erforderlich zur Umsetzung ist eine enge und kontinuierliche Zusammenarbeit und Abstimmung zwischen dem Versicherer und den Dienstleistern sowie deren Datenschutzabteilungen, um gegenseitigen Aufwand möglichst zu minimieren und nicht praktikable Anforderungen zu vermeiden. Die Praxis zeigt: „Es geht, aber nur gemeinsam."

Thomas Fenstermacher ist Vorstandsvorsitzender der servicekonzept AG. RA Dr. Karsten Kinast LL.M. ist Datenschutzbeauftragter und berät Unternehmen bei Datenschutzkonzepten.

BWV-Datenschutz zertifiziert

Das internationale Zertifikat nach ISO IEC 27001 ist jetzt dem Geschäftsbereich Außendienst-Ausbildung des Berufsbildungswerks der Deutschen Versicherungswirtschaft (BWV) in Köln verliehen worden. Für das BWV, das deutschlandweit als Dienstleister der Industrie- und Handelskammern die Durchführung der Sachkundeprüfung „Geprüfte/r Versicherungsfachmann/-frau IHK" unterstützt, hat das Thema „Informationssicherheit" gerade im Bereich der Kundenbeziehungen große Bedeutung. Die Kontrolle über Informationen und Daten im Sinne der Verfügbarkeit, Vertraulichkeit und Integrität muss in klar strukturierten Prozessen verlaufen. Daher hat das BWV das Informations-Sicherheits-Managementsystem eingeführt. Die ISO-Norm gilt weltweit als Benchmark für Verwaltung und Schutz wertvoller Informationsressourcen. Sie dokumentiert Qualität und Sicherheit in Bezug auf jegliche Form von Daten und Informationen im Unternehmen. Das Zertifikat wurde von der Dekra Certification GmbH ausgestellt. Während des Zertifizierungsprozesses wurde das BWV vor Ort geprüft, die Prozessabläufe untersucht und der gesamte Geschäftsablauf auditiert. Um die Konstanz zu sichern, werden in regelmäßigen Abständen Rezertifizierungen durchgeführt. VW