rung. Dennoch sind bereits Arbeiten in Bezug auf eine Teilrevision der neuen Aufsichtsverordnung im Gange: Das Ausmass der Unwetterschäden des vergangenen Sommers lässt eine Erhöhung der Deckungen für die Versicherung von Fahrhabe und Gebäude gegen Elementarereignisse von heute 250 Millionen Franken auf je 1 Mia. Franken als notwendig erscheinen. Gleichzeitig werden bei diesen Arbeiten u.a. auch die Selbstbehaltregelungen, die seit mehr als 20 Jahren weitgehend unverändert gelten, an die heutigen Verhältnisse angepasst. Die Teilrevision AVO soll voraussichtlich per 1. Januar 2007 in Kraft treten.

Revision des Datenschutzgesetzes – Compliance-Herausforderungen für die Versicherer

Thomas Müller*

Am 26. März 2006 verabschiedeten die eidgenössischen Räte eine Teilrevision des Datenschutzgesetzes (DSG)[1]. Wegen der Entwicklung der elektronischen Datenbearbeitung soll das informationelle Selbstbestimmungsrecht der betroffenen Personen verstärkt werden. Der Gesetzgeber versuchte gleichzeitig, einen angemessenen Ausgleich zwischen den Interessen der betroffenen Personen[2] und jenen der Inhaber von Datensammlungen zu schaffen. Die Umsetzung der neuen Gesetzesbestimmung stellt für die Versicherer eine Compliance[3]-Herausforderung dar. Nachfolgend werden die wichtigsten neuen Bestimmungen aus der Sicht der Versicherer dargestellt.

I. Verstärkung des Transparenzgebotes[4]

Das Transparenzgebot[5] erfährt im revidierten Datenschutzrecht in zweifacher Hinsicht eine Konkretisierung: Es gilt nicht nur für die Datenbeschaffung[6], sondern generell für die Datenbearbeitung. Weiter verlangt Art. 4 Abs. 4 nDSG ausdrücklich, dass die Beschaffung der Personendaten und insbesondere der Zweck der Bearbeitung für die betroffene Person er-

* Fürsprecher, Zürich.

1 Bundesgesetz über den Datenschutz (DSG; SR 235.1), Änderungen vom 24. März 2006, BBl 2006, 3547 ff. Bis zum Ablauf der Referendumsfrist wurde kein Referendum ergriffen.

2 Art. 3 lit. b DSG: Unter dem Begriff der betroffenen Person werden die natürlichen und juristischen Personen verstanden, über die Daten bearbeitet werden.

3 Compliance umfasst die Aufgabe und die Funktion, in einer Unternehmung die Voraussetzungen und das Bewusstsein zu schaffen, dass alle Mitarbeitende sämtliche, für die Unternehmung relevanten Bestimmungen einhalten und einhalten können. Zudem ist Compliance verantwortlich, für die Einhaltung der relevanten Bestimmungen sowie für die notwendige Kontrolle besorgt zu sein. Aus: Outsourcing von Compliance, Möglichkeiten und Grenzen, Gruppenarbeit, eingereicht im 4. Lehrgang NDK Compliance Management, Institut für Finanzdienstleistungen Zug (IFZ) am 15. Mai 2004 bei Frau Dr. iur. Monika Roth.

4 Motion "Erhöhte Transparenz" 00.300 vom 28.1.2000 der Kommission für Rechtsfragen des Ständerates, die von den eidgenössischen Räten am 5.10.2000 gutgeheissen worden ist.

5 Urs Maurer, in: Urs Maurer/Nedim Peter Vogt (Hrsg.), Basler Kommentar zum schweizerischen Datenschutzgesetz, Art. 4 N 8. Der Grundsatz des informationellen Selbstbestimmungsrechts ist schon heute in Art. 4 Abs. 2 DSG festgeschrieben.

6 BKS DSG-maurer (Fn 5), Art. 4 N 7 leitete aus der Systematik von Art. 4 Abs. 1 und Art. 4 Abs. 2 DSG bereits für das geltende Recht den Grundsatz ab, dass sich die Rechtmässigkeit sowohl auf die Datenbeschaffung als auch auf die Datenbearbeitung beziehen muss.

kennbar sein müssen. Dieser Grundsatz galt bisher nur für Bundesorgane[7] und wird nun neu auf die privaten Personen als Inhaber von Datensammlungen ausgedehnt. Die Anforderungen an die Erkennbarkeit der Datenbeschaffung sind nach den konkreten Umständen sowie nach den Grundsätzen der Verhältnismässigkeit und von Treu und Glauben zu beurteilen.

Art. 4. Abs. 5 nDSG klärt den bereits heute bekannten Begriff[8] der Einwilligung der betroffenen Person zur Datenbearbeitung. Grundsätzlich muss die Einwilligung nach einer angemessenen Information freiwillig erfolgen. Die Zustimmung muss umso klarer erfolgen, je sensibler die fraglichen Personendaten sind[9]. Die Einwilligung der betroffenen Person erfolgt in einer graduellen Abstufung: Die Einwilligung kann stillschweigend beziehungsweise durch konkludentes Verhalten erfolgen. Sofern es sich jedoch um besonders schützenswerte Daten wie Gesundheits- oder Sanktionsdaten handelt, muss die Einwilligung ausdrücklich erfolgen.

Das Element der Freiwilligkeit der Erteilung der Zustimmung erfährt dadurch eine starke Einschränkung, dass die versicherte Person nur zwischen dem Erteilen der Zustimmung und somit zum Beispiel einer speditiven Schadenregulierung oder einer Verweigerung der Zustimmung und somit einer langwierigen Schadenregulierung wählen kann, da der Versicherer auf eine Informationsbeschaffung angewiesen ist. Das bedeutet insbesondere, dass der Versicherer die betroffene Person über die möglichen negativen Folgen oder Nachteile, die sich aus der Verweigerung ihrer Zustimmung ergeben können, im Voraus und aktiv informieren muss[10]. Die alleinige Tatsache, dass eine Verweigerung einen Nachteil für die betroffene Person nach sich zieht, kann die Gültigkeit der Zustimmung jedoch nicht beeinträchtigen, solange der Nachteil verhältnismässig ist.

Aufgrund der neuen Bestimmung von Art. 4 Abs. 5 nDSG ist davon auszugehen, dass die Versicherer die Einwilligungserklärungen zur Beschaffung und zur Bearbeitung von besonders schützenswerten Daten derart anzupassen haben, dass für die betroffene Person mindestens der Kreis der Dritten erkennbar ist, bei denen Daten beschafft werden, respektive an welche Daten weitergeleitet werden. Die Schwierigkeit der Umsetzung dieser Anforderung wird darin liegen, dass zum Beispiel bei Beginn der Schadenregulierungsarbeiten noch gar nicht abschliessend klar ist, bei welchen Dritten medizinische Daten im Sinne der besonders schützenswerten Daten über die versicherte Person eingeholt werden müssen. Somit lässt sich eine Verzögerung und Komplizierung der Schadenregulierung leider nicht vermeiden, da unter Umständen eine weitere Einwilligungserklärung eingeholt werden muss. Zusätzlich empfiehlt es sich, die Einwilligungserklärung zur Datenbeschaffung von besonders schützenswerten Daten bei Dritten[11] mit der Information[12] zu ergänzen, dass bei den namentlich genannten Dritten besonders schützenswerte Daten eingeholt werden, und den Zweck der Datenbearbeitung[13] bekanntzugeben, sofern er nicht bereits aus den Umständen ersichtlich ist (z.B. beim Schadenanmeldeformular ist für die betroffene Person ersichtlich, dass die erhobenen Daten zur Schadenregulierung verwendet werden).

II. Datenbearbeitungsgrundsätze

Die Datenbearbeitungsgrundsätze des bisher geltenden DSG erfahren aufgrund der Revision keine grundlegenden Änderungen. Einige Vorschriften wurden aufgrund von Lehre und Rechtsprechung konkretisiert.

Mit der Verschiebung von Art. 14 aDSG in Art. 10a nDSG und somit in den allgemeinen Teil des DSG findet diese Bestimmung über die Datenbearbeitung durch Dritte neu auch auf Bundesorgane[14] Anwendung. Die Bearbeitung von Daten kann einem Dritten nur übertragen werden, wenn die Datensicherheit gewährleistet ist[15] und sich der Versicherer überdies darüber vergewissert, dass diese Datensicherheit durch den Dritten gewährleistet ist. Bei der Übertragung der Datenbearbeitung an aussenstehende Dritte muss der Versicherer ausdrücklich eine Vereinbarung[16] abschliessen und darin sämtliche Datenschutzverpflichtungen an den Beauftragten überbinden. Deshalb muss der Versicherer den Beauftragten vor Vertragsabschluss auf die Einhaltung der schweizerischen Datenschutzgrundsätze überprüfen. Der Versicherer hat jedoch auch während der Dauer des Vertrages periodische Kontrollen beim Beauftragten durchzuführen, ob die Voraussetzungen gemäss Art. 10a nDSG noch gegeben sind.

7 Art. 18 DSG.
8 Bereits das geltende Recht verwendet diesen Begriff z.B. in Art. 13 Abs. 1 DSG, Art. 17 Abs. 2 lit. c DSG.
9 Lucas S. Brühwiler-Frésey, Medizinischer Behandlungsvertrag und Datenschutz, Zürich 1996, 87.
10 BBl 2003, 2127.
11 Art. 7a Abs. 3 nDSG.
12 Art. 7a Abs. 1 nDSG.
13 Art. 7a Abs. 2 nDSG.
14 Dies wirkt sich dort aus, wo ein Versicherer das KVG oder das UVG betreibt.
15 BBl 2003, 2135.
16 Art. 10a Abs. 1 nDSG.

Auch im neuen Recht dürfen Personendaten grundsätzlich nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung zur Gewährleistung eines angemessenen Schutzes fehlt. Dennoch erfuhren die Grundlagen der grenzüberschreitenden Datenbearbeitung eine markante Vereinfachung. Da sich die bisherige Meldepflicht bei der Bekanntgabe von Personendaten ins Ausland gem. Art. 6 aDSG nicht bewährt hat[17], wird neu eine Sorgfaltspflicht eingeführt. Falls im Empfängerstaat eine Gesetzgebung fehlt, die einen angemessenen Datenschutz gewährleistet, darf eine Datenbekanntgabe ins Ausland nur erfolgen, sofern die in Art. 6 Abs. 2 nDSG abschliessend aufgezählten, alternativen Bedingungen[18] eingehalten werden. In diesem Sinne sind beim Versicherer Prozesse aufzubauen, die bei der Datenübertragung ins Ausland die Einhaltung der Sorgfaltspflichten gem. Art. 6 Abs. 2 nDSG gewährleisten. Aus Gründen der Beweisbarkeit und der Risikoabwägung empfiehlt es sich, bei der Datenübertragung ins Ausland in Anwendung von Art. 10a nDSG eine Vereinbarung mit dem Beauftragten respektive mit dem Empfänger der Daten im Ausland abzuschliessen. Aufgrund der Ausführungen in der Botschaft des Bundesrates[19] ist davon auszugehen, dass es sich bei der Information an den eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten[20] (EDÖB) um eine einmalige Mitteilung handelt, dass der Versicherer die internen Prozesse den neuen Bestimmungen gemäss Art. 6 nDSG angepasst hat.

III. Register der Datensammlungen

Grundsätzlich bleibt das System bestehen, dass Bundesorgane (und somit auch Versicherer, die das KVG und das UVG betreiben) sowie private Personen, die besonders schützenswerte Daten bearbeiten oder Daten an Dritte bekannt geben, die entsprechenden Datensammlungen beim EDSB anmelden müssen[21]. Hingegen hat eine Anmeldung bei Vorliegen einer der Bedingungen gemäss Art. 11 Bst. a Abs. 5 nDSG nicht zu erfolgen. Folgedessen ist keine Anmeldung vorzunehmen, wenn der Versicherer einen Datenschutzverantwortlichen bezeichnet hat, der über die Einhaltung der datenschutzrechtlichen Rahmenbedingungen wacht[22]. In der Botschaft des Bundesrates wird dazu ausgeführt, dass der Datenschutzverantwortliche organisatorisch unabhängig sein muss, d.h., er darf bezüglich der Datenschutzangelegenheiten nicht weisungsgebunden oder hierarchisch untergeordnet sein. Ebenso entfällt die Pflicht zur Anmeldung, wenn der Versicherer eine Zertifizierung gem. Art. 11 nDSG vorgenommen hat[23]. Diese Befreiungsgründe von der Anmeldepflicht gelten für die Versicherer unabhängig davon, ob sie das Privatversicherungsgeschäft, das Unfall- oder Krankenversicherungsgeschäft (als Bundesorgane) betreiben.

IV. Zertifizierungsverfahren

Mit der Teilrevision des DSG soll die Selbstregulierung[24] auch im Bereiche des Datenschutzes gefördert werden. Hersteller von Datenbearbeitungssystemen oder -programmen sowie private Personen oder Bundesbehörden können ihre Systeme, Verfahren und ihre Organisation einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen[25]. Das Zertifizierungssystem soll zur Vergabe eines Datenschutz-Qualitätszeichens führen[26]. Es wird sich erst nach Vorliegen der vom Bundesrat zu erlassenden Ausführungsverordnung weisen, welche Auswirkungen diese Bestimmung in der Praxis zeitigt.

V. Rechtsschutz

Der Rechtsschutz der betroffenen Person wird nur insofern erweitert, als dass im Rahmen von Auskunftsersuchen gem. Art. 8 nDSG neu auch die verfügbaren Angaben über die Herkunft der Daten angegeben werden müssen[27]. Die Angabe der Herkunft der Daten kann in der Regel bereits heute aufgrund des Absenders oder des Verfassers der gespeicherten Daten gemacht werden.

[17] BBl 2203, 2128.
[18] BBl 2003, 2128.
[19] BBl 2003, 2130.
[20] Der Eidgenössische Datenschutzbeauftragte erhält eine neue Funktion: Am 1. Juli 2006 übernimmt er im Rahmen des Bundesgesetzes über das Öffentlichkeitsprinzip in der Verwaltung, kurz Öffentlichkeitsgesetz genannt, die Aufgabe als Beratungs- und Schlichtungsorgan. Neu heisst er Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB.
[21] Christian Drechsler, Notifikationspflichten unter revidiertem DSG, digma, Zeitschrift für Datenrecht und Informationssicherheit 2006/2, 90 ff.
[22] BBl 2003, 2138.
[23] Art. 11 Abs. 5 lit. f nDSG.
[24] Im Bereiche der Bekämpfung der Geldwäscherei wurde für die Einhaltung der Gesetzesbestimmungen und deren Überwachung mit dem Bundesgesetz vom 10. Oktober 1997 zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG; SR 955.00) die Selbstregulierung zum Standard erhoben. Siehe dazu Art. 24 ff. GwG.
[25] Art. 11 nDGS.
[26] BBl 2003, 2136.
[27] Art. 8 Abs. 2 lit. b nDSG.