Stellungnahme

zum Vorschlag der EU-Datenschutzverordnung

KOM(2012) 11/4

vom 25. Januar 2012

Zusammenfassung

Die Deutsche Versicherungswirtschaft unterstützt die Ziele, das Datenschutzrecht in Europa zu vereinheitlichen, die grenzüberschreitende Tätigkeit zu erleichtern und Hemmnisse für den internationalen Datentransfer zu beseitigen. Die Idee des „One-stop-shops“ sollte ausgebaut werden.

Angesichts des ohnehin schon hohen Datenschutzstandards z. B. in Deutschland sollte eine Regelung der Rechte der Betroffenen und der Anforderungen an Datenschutz und Datensicherheit jedoch mit Augenmaß erfolgen und unnötige bürokratische Belastungen vermeiden. Regelungen, die erkennbar von Vorfällen in der Internetwirtschaft angestoßen sind und nur für den Bereich des Internets Sinn ergeben, sollten dabei nicht generell und allgemeingültig gemacht werden.

Im Hinblick auf versicherungsspezifische Geschäftsabläufe enthält der Vorschlag der Datenschutz-Grundverordnung noch erhebliche rechtliche Unsicherheiten sowie Bestimmungen, die die Bereitstellung von Versicherungsschutz erheblich erschweren, verteuern und in Teilen sogar gefährden würden.

Die zukünftige Verordnung sollte insbesondere folgende Punkte berücksichtigen:

- Es bedarf einer eindeutigen **Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten** in der Lebens-, Kranken-, Unfall- und Haftpflichtversicherung und Rückversicherung. Sie muss auch inzwischen gebräuchliche und sinnvolle **Datenverarbeitungen im Konzern und unter Beteiligung spezialisierter Dienstleister** erfassen (dazu Ziffer 1).

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5290
Fax: +49 30 2020-6290

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +32 2 28247-39

Ansprechpartner:
Dr. Martina Vomhof
Leiterin
Datenschutz/Grundsatzfragen

E-Mail: m.vomhof@gdv.de

www.gdv.de

- Tarifierung und Risikodifferenzierung als Kernbestandteile des Versicherungsgeschäfts müssen möglich bleiben. Die auf das Internet zugeschnittenen Bestimmungen zur **Profilbildung** (Art. 20) dürfen die Tarifeinstufung und Risikoeinschätzung in der Versicherungswirtschaft nicht erfassen. Die **Begriffsbestimmungen** müssen dahingehend überarbeitet werden, dass die Nutzung weniger sensibler Sachdaten und pseudonymisierter Daten möglich bleibt. (dazu Ziffer 2).
- Verfahren zum **Schutz vor Versicherungsbetrug und unzuverlässigen Versicherungsvermittlern** müssen durchführbar bleiben (dazu Ziffer 3).
- Umfangreiche **Betroffenenrechte**, wie das Recht auf Vergessen (Art. 17) und Datenübertragbarkeit (Art. 18), die primär auf soziale Netzwerke im Internet zugeschnitten sind, dürfen die Vertragsdurchführung nicht gefährden (dazu Ziffer 4).
- Die **Anforderungen an Maßnahmen zu Datenschutz und Sicherheit** müssen praktikabel bleiben (dazu Ziffer 5). Die erheblich belastende Datenschutz-Folgenabschätzung (Art. 33) sollte entfallen und die Verpflichtung zur Meldung von Datenpannen auf gravierende Fälle eingeschränkt werden (Art. 31, 32).
- Möglichkeiten zur **kollektiven Rechtsdurchsetzung** sind nicht erforderlich, zumal den Datenschutzaufsichtsbehörden weitgehende Kompetenzen eingeräumt sind (dazu Ziffer 7). **Sanktionen** sollten auf ein verträgliches Maß begrenzt werden (Ziffer 8).
- Die weiten Befugnisse der Europäischen Kommission zum **Erlass von delegierten Rechtsakten** bedeuten Rechtsunsicherheit. Vorzugswürdig ist eine Konkretisierung der Verordnung durch branchenspezifische **Selbstregulierungsmaßnahmen** (dazu Ziffer 9).

Inhaltsübersicht

Vorbemerkung

Als Risikoträger für Unternehmen und private Haushalte erfüllt die Versicherungswirtschaft im Rahmen der gesamten Volkswirtschaft eine essentielle Funktion. Ebenso wie individuelle Eigenvorsorge oder eine staatliche Absicherung zählt die Möglichkeit, sich über einen privaten Versicherungsschutz gegen elementare Lebensrisiken abzusichern, in der sozialen Marktwirtschaft zu den Eckpfeilern der Daseinsvorsorge. Indem die Versicherungswirtschaft private oder öffentliche Risiken übernimmt, schafft sie für Unternehmen und Wirtschaft die Sicherheiten, die notwendig sind, damit sich Initiative und innovatives Unternehmertum überhaupt erst entfalten können. Die Absicherung gegen private Lebensrisiken ermöglicht den Bürgerinnen und Bürgern ein Leben in Freiheit und Sicherheit.

Allein in Deutschland bieten Versicherungsunternehmen mit ca. 450 Millionen Versicherungsverträgen umfassenden Risikoschutz und soziale Sicherheit.

Die deutschen Versicherer sind sich ihrer Verantwortung bewusst, die damit einhergeht, dass sie zur Erfüllung ihrer Aufgaben personenbezogene Daten ihrer Kunden und Antragsteller verarbeiten müssen. Aus diesem Grund erarbeitet der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) zurzeit gemeinsam mit den deutschen Datenschutzbehörden aktuell Verhaltensregeln zum Umgang mit personenbezogenen Daten (Code of Conduct). In engem Zusammenhang mit dieser geplanten Selbstregulierungsmaßnahme steht eine gemeinsam erarbeitete datenschutzrechtliche Einwilligungsklausel für die Lebens- und Krankenversicherung, die seit Januar 2012 von den deutschen Datenschutzbehörden empfohlen wird und auch die nach deutschem Strafrecht geforderte Schweigepflichtentbindung umfasst. Auch der Verbraucherzentrale Bundesverband (vzbv) als wichtigste Interessenvertretung der Verbraucher in Deutschland ist an der Ausarbeitung des Code of Conduct und der Einwilligung beteiligt. Die Versicherungswirtschaft wird damit in Deutschland als erste Branche ein Datenschutzkonzept haben, das von Datenschutzbehörden, Verbraucherschützern und Wirtschaft gemeinsam getragen wird.

Vor diesem Hintergrund begrüßt die deutsche Versicherungswirtschaft das Bestreben der Europäischen Kommission, das Datenschutzrecht in Europa zu vereinheitlichen. Für europaweit tätige Unternehmen bedeutet es eine erhebliche Erleichterung, wenn sie sich nicht mit unterschiedlichen materiellen Datenschutzvorschriften auseinandersetzen müssen.
Anreize zur Implementierung von Codes of Conduct (Art. 38) und Binding Corporate Rules (Art. 43) sind sinnvoll. Jedoch sollten die Anforderungen an den Inhalt nicht zu starr festgelegt werden, um eine breite Akzeptanz und Praktikabilität zu sichern.

Aus Sicht der Versicherungswirtschaft sollte die zukünftige Verordnung insbesondere folgende Punkte berücksichtigen:

1. Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft

a) Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten

Es bedarf einer eindeutigen Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten in der Lebens-, Kranken, Unfall- Haftpflicht- und Rückversicherung.

Hintergrund:

In der Krankenversicherung, in der Lebensversicherung und in der Unfallversicherung werden Gesundheitsdaten zwingend benötigt, um im Einklang mit versicherungsaufsichtsrechtlichen Bestimmungen die zu versichernden Risiken zu prüfen und um Versicherungsfälle abwickeln zu können.

Beispiele:

- Es kann nur festgestellt werden, ob ein Versicherter Anspruch auf eine Berufsunfähigkeitsrente hat, wenn geprüft worden ist, ob er eine Erkrankung hat, aufgrund derer er seinen Beruf nicht mehr ausüben kann.
- Ein Krankenrücktransport aus dem Ausland kann nur organisiert werden, wenn dem Versicherer oder Assisteur, der den Transport organisiert, bekannt ist, welche Erkrankung der Versicherte hat.
- Rückversicherer, die Risiken von den Erstversicherern ganz oder teilweise übernehmen und damit die Erfüllung der Verträge sicherstellen, benötigen Gesundheitsdaten, um zu prüfen, ob sie das Risiko zeichnen können bzw. im Versicherungsfall dafür einstehen müssen.
- Haftpflichtversicherer können Personenschäden nur abwickeln, wenn sie die Gesundheitsdaten der Geschädigten verarbeiten können.

Ziel muss es sein, die für die soziale Absicherung der Bevölkerung notwendige Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft auf eine rechtssichere Grundlage zu stellen. Sie muss den Interessen der Versicherten und Antragsteller Rechnung tragen, zu denen auch effiziente Prozessabläufe im Rahmen von Risikoprüfung und Schadenabwicklung zählen.

Verordnungsvorschlag der Kommission:

Der Vorschlag enthält bisher **keine ausreichende gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft**. Eine solche gesetzliche Grundlage ist für die Versicherungsbranche – auch nach Überzeugung der deutschen Datenschutzbehörden – dringend erforderlich.

Der Vorschlag enthält zwar viele Ansatzpunkte, die eine **gesetzliche Grundlage** für die notwendige Verarbeitung von Gesundheitsdaten bieten könnten. Jedoch reichen sie nicht aus:

- Art. 9 Abs. 2f) regelt die Verarbeitung zur Begründung, Geltendmachung oder Abwehr von Rechtsansprüchen, nicht aber (wie Art. 6 Abs. 1b) zur Begründung und Durchführung von Verträgen.
- Art. 9 Abs. 2g) dürfte vermutlich nicht angewendet werden, wenn Art. 9 Abs. 2h) i. V. m. Art. 81 der Verordnung als spezielle Erlaubnisnormen für die Verarbeitung von Gesundheitsdaten verstanden werden.
- Nach Art. 9 Abs. 2h) ist die Verarbeitung von Gesundheitsdaten zulässig, wenn sie vorbehaltlich der Bedingungen und Garantien des Art. 81 für „*Gesundheitszwecke*" erforderlich ist. Damit ist allenfalls die Krankenversicherung erfasst. Inwiefern dies der Fall ist, ist angesichts der Formulierung des Art. 81 Abs. 1c zudem unsicher.

Die Nutzung von **Einwilligungen** als Rechtsgrundlage kann nur eine Notlösung sein. Sie wird den tatsächlichen Geschäftsabläufen nicht gerecht und führt im Ergebnis zu einer Verschlechterung der Situation der Versicherungsnehmer.

Der Vorschlag geht davon aus, dass die betroffene Person eine völlige Entscheidungsfreiheit hat und ihre **Einwilligung jederzeit widerrufen** kann (Art. 7 Abs. 3 und Erwägungsgrund 32). Wenn die Daten zur Durchführung eines Vertrages verarbeitet werden müssen, kann der Kunde theoretisch zwar auf den Vertragsschluss verzichten. Eine Vertragsdurchführung ohne Verarbeitung der Daten ist aber nicht möglich. Bei der inzwischen üblichen Datenverarbeitung in vorgegebenen automatisierten Prozessen, die der Abwicklung von Millionen von Verträgen dient, ist es auch nicht realistisch, dass einzelne Betroffene die Art und Weise der Verarbeitung beeinflussen können.

Die Zulässigkeit der Einwilligungen in der Versicherungswirtschaft wird zudem durch **Art. 7 Abs. 4** des Verordnungsvorschlags infrage gestellt. Danach ist die **Einwilligung** als Rechtsgrundlage der Datenverarbeitung **ausgeschlossen**, wenn zwischen dem Betroffenen und der verantwortlichen Stelle ein **erhebliches Ungleichgewicht** besteht. Nach Erwägungsgrund 34 ist dies der Fall, wenn ein Abhängigkeitsverhältnis besteht, z. B. in Beschäftigungsverhältnissen. Nach der Einschätzung von Datenschutzbehörden ist es auszuschließen, dass ein solches Ungleichgewicht nicht nur zwischen Arbeitgebern und Arbeitnehmern, sondern auch zwischen Versicherungsunternehmen und ihren Kunden oder Geschädigten angenommen wird. Damit wäre eine Einwilligung ausgeschlossen. Ein genereller Ausschluss der Einwilligung in Art. 7 Abs. 4 schränkt Verbraucher in ihrer Entscheidungsfreiheit ein und steht dem eigentlichen Ziel des Datenschutzes entgegen, den Einzelnen als Herrn über seine Daten zu stärken. Die Versicherungswirtschaft stellt er vor große Schwierigkeiten, ihre Datenverarbeitung zu rechtfertigen.

Position der deutschen Versicherungswirtschaft:

Notwendig ist eine eindeutige, europaweit geltende gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten in allen betroffenen Versicherungssparten, also in der Lebens-, Kranken-, Unfall- und Haftpflichtversicherung sowie bei Rückversicherungen. Eine solche gesetzliche Grundlage muss sich auch auf die unternehmensübergreifende Datenverarbeitung im Konzern sowie die Einschaltung von dritten Personen, wie z. B. ärztlichen Gutachtern und Assistance-Unternehmen, erstrecken (dazu unten 2).

Vorschlag der deutschen Versicherungswirtschaft:

Art. 9 Abs. 2 h) sollte wie folgt gefasst werden:

> ***„die Verarbeitung betrifft Gesundheitsdaten und ist vorbehaltlich der Bedingungen und Garantien des Art. 81 oder Art. 81a ~~für Gesundheitszwecke~~ erforderlich oder“***

Es sollte ein **neuer Art. 81 a Abs. 1** eingefügt werden:

> ***„Die Verarbeitung von Gesundheitsdaten ist zulässig, wenn sie für die Erfüllung eines Versicherungsvertrages einschließlich der Rückversicherung oder eines gesetzlichen Haftungsanspruchs, zur Identifizierung erhöhter Risiken oder zum Schutz vor Versicherungsbetrug durch ein Erst- oder Rückversicherungsunternehmen erforderlich ist.“***

Art. 7 Abs. 4 *muss unbedingt* ***gestrichen*** *werden.*

b) Verarbeitung von Gesundheitsdaten im Konzern und Beteiligung von Dienstleistern

Es bedarf einer Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten im Konzern und Beteiligung von Dienstleistern.

Hintergrund:

Um Synergien zu erzielen und dem Gebot der Wirtschaftlichkeit zu entsprechen, müssen innerhalb von Versicherungsgruppen ebenso wie in anderen Branchen Serviceaufgaben delegiert und zentralisiert oder an kompetente Dienstleister ausgelagert werden.

Beispiele:

- Die Entgegennahme von Schadensmeldungen, die Überwachung der Schadensabwicklung sowie die Steuerung von Gutachtenaufträgen wird

von einem bestimmten Konzernunternehmen oder einem spezialisierten Dienstleister übernommen.

- Ein Unternehmen überträgt die gesamte Risikoprüfung und Schadensbearbeitung für alle Konzerngesellschaften Mitarbeitern der Konzernmutter.
- Erkrankungen werden z. B. in kleineren Gesellschaften immer und bei großen Unternehmen in bestimmten Fällen durch externe Ärzte begutachtet.
- Eine Krankenversorgung im Ausland und Krankenrücktransporte werden durch hierauf spezialisierte Assistance-Gesellschaften durchgeführt.
- Die Versorgung mit medizinischen Hilfsmitteln erfolgt durch Fachbetriebe.

Sowohl diese Maßnahmen als auch die Risikoverlagerung auf Rückversicherer sind nach der Richtlinie 2009/138/EG des Europäischen Parlamentes und des Rates vom 25. November 2009 (betreffend die Aufnahme und Ausübung der Versicherungs- und Rückversicherungstätigkeit – Solvency II) versicherungsaufsichtsrechtlich zulässig.

Vorschlag der Kommission:

Art. 4 Abs. 5 und Art. 24 sind für die Regelung der gemeinsamen Datenverarbeitung nicht hilfreich, weil sie keine eindeutige Ermächtigungsgrundlage für eine Datenweitergabe von einer verantwortlichen Stelle an die andere schaffen. Sobald eine gesamte Aufgabe übertragen wird, liegt nach Auffassung vieler Datenschutzbehörden keine Auftragsdatenverarbeitung vor, sodass Art. 26 nicht eingreift.

Wenn Gesundheitsdaten verarbeitet werden, bedarf es somit grundsätzlich für jede Datenübermittlung einer **Einwilligung** des Betroffenen. Abgesehen von den erheblichen rechtlichen Unsicherheiten einer solchen Einwilligung (dazu oben 1a) und dem damit verbundenen Zeit- und Kostenaufwand erweist sich dieser Weg für alle Veränderungen während der Laufzeit eines Versicherungsvertrages als äußerst unpraktikabel. Nach Abschluss des Vertrages reagiert die Mehrzahl der Betroffenen auf die Bitte zur Abgabe der Erklärung erfahrungsgemäß schlichtweg nicht. Es ist nicht möglich, angesichts notwendiger Veränderungen der Geschäftsprozesse immer wieder jeden einzelnen Versicherungsnehmer erneut um seine Einwilligung zu bitten.

Die Probleme können in der Versicherungswirtschaft nicht einfach gelöst werden, indem Unternehmen zusammengelegt und damit zu einer einheitlichen verantwortlichen Stelle gemacht werden. Denn Versicherungsunternehmen sind gemäß Art. 73 der Richtlinie 2009/138/EG grundsätzlich zur **Spartentrennung** zwischen Lebens- und Nichtlebensversicherung verpflichtet. Diese Versicherungssparten dürfen nur durch verschiedene juristische Personen betrieben werden. In Deutschland gilt das Spartentrennungsgebot zudem für die substitutive Krankenversicherung und für die Leistungsbearbeitung in der Rechtsschutzversicherung. Diese Re-

geln dienen nur der Trennung der Haftungsmassen, haben aber keinen datenschutzrechtlichen Grund.

Position der deutschen Versicherungswirtschaft:

Anstelle einer Einwilligung, die von vielen Betroffenen ohne Reflektion abgegeben wird und daher oft keinen besonderen Schutz bietet, sollten gesetzliche Anforderungen an die Zulässigkeit der Datenübermittlung zwischen Unternehmen einer Versicherungsgruppe, an Rückversicherungsunternehmen und an Dienstleister geschaffen werden. Wenn sichergestellt ist, dass die Daten nur dem ursprünglichen Zweck entsprechend verarbeitet werden, dass die anderen Unternehmen unter Berücksichtigung der Eignung der von ihnen zu Datenschutz und Datensicherheit getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt sind und dazu vertraglich vereinbart wurde, dass der Geheimnis- und Datenschutz bei dem anderen Unternehmen gewährleistet ist, muss auch eine Übermittlung von Gesundheitsdaten zulässig sein.

Mit dieser gesetzlichen Lösung würden alle Betroffenen geschützt, unabhängig davon, ob sie eine Einwilligung erteilen oder nicht.

Vorschlag der deutschen Versicherungswirtschaft:

Es sollte ein **neuer Art. 81 a Abs. 2** eingefügt werden:

> ***„Soweit ein Erst- oder Rückversicherungsunternehmen einem anderen Unternehmen oder Personen im Rahmen von Satz 1 Daten zur Verarbeitung im Auftrag oder zur eigenverantwortlichen Erfüllung von Datenverarbeitungs- oder sonstigen Aufgaben überlässt, ist die Weitergabe und anschließende Verarbeitung dieser Daten zu dem von dem Erst- oder Rückversicherungsunternehmen bestimmten Zweck ohne Einwilligung des Betroffenen unter den nachfolgenden Voraussetzungen zulässig. Die anderen Unternehmen oder Personen sind unter Berücksichtigung der Eignung der von ihnen zu Datenschutz und Datensicherheit getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen und es ist vertraglich zu vereinbaren, dass der Geheimnis- und Datenschutz bei dem anderen Unternehmen oder Personen gewährleistet ist wie bei dem Erst- oder Rückversicherungsunternehmen selbst.“***

c) Verarbeitung von genetischen und biometrischen Daten in der Versicherungswirtschaft

aa) Genetische Daten

Die im Versicherungsgeschäft notwendige Verarbeitung von genetischen Daten im muss auf sicherer Rechtsgrundlage möglich sein.

Hintergrund:

Die deutschen Versicherer verlangen weder vor noch nach Abschluss eines Versicherungsvertrages die Durchführung genetischer Untersuchungen. Auf die Ergebnisse vorhandener genetischer Untersuchungen wird im Rahmen des gesetzlich Zulässigen nur bei Abschluss von Verträgen mit sehr hohen Beitragssummen zurückgegriffen. Möglich bleiben muss jedoch die Anzeige bekannter Vorerkrankungen nach Maßgabe des jeweils geltenden Versicherungsvertragsrechts.

Im Rahmen ärztlicher Diagnosen spielt heute neben konventionellen Untersuchungsmethoden häufig die Auswertung genetischer Daten eine Rolle. Welche Art von Krebserkrankung besteht und wie sie behandelt werden kann, kann z. B. konventionell, aber auch anhand genetischer Untersuchungen festgelegt werden. Die Versicherungswirtschaft benötigt Untersuchungsergebnisse für die Risikoprüfung und Leistungsbearbeitung in der Personenversicherung. Die Nutzung der Daten für die Prüfung einer bestehenden, diagnostizierten Erkrankung darf nicht davon abhängen, welche Untersuchungsmethode ein Arzt zugrunde legt.

Verordnungsvorschlag der Kommission:

Nach Art. 4 Abs. 10 sind „genetische Daten“ Daten jedweder Art zu den ererbten oder während der vorgeburtlichen Entwicklung erworbenen Merkmalen eines Menschen. Dieser Begriff der genetischen Daten ist zu weit. Er erfasst z. B. auch das für jedermann sichtbare Geschlecht. Außerdem werden Behinderungen erfasst, die nicht genetisch bedingt sind, sondern während der Schwangerschaft der Mutter, z. B. durch Sauerstoffmangel, erworben wurden.

Art. 9 Abs. 1 bezieht auch „genetische Daten“ in die besonderen Kategorien personenbezogener Daten ein, ohne jedoch hinreichende Ausnahmen festzulegen.

Position der deutschen Versicherungswirtschaft:

Der Begriff der „genetischen Daten“ in Art. 4 Abs. 10 sollte auf mit Untersuchung der DNA, RNA oder der Chromosomen gewonnenen Daten über genetische Eigenschaften eines Menschen begrenzt werden.
Die Nutzung genetischer Daten für die Prüfung einer bestehenden, diagnostizierten Erkrankung muss aber ebenso möglich sein wie die Nutzung der Ergebnisse konventioneller Untersuchungsmethoden, da nicht beeinflussbar ist, welchen Methoden ein Arzt zugrunde legt. Insofern sollten genetische Daten wie Gesundheitsdaten behandelt werden.

Vorschlag der deutschen Versicherungswirtschaft:

Art. 4 Abs. 10 sollte wie folgt neu gefasst werden:

> ***„Genetische Daten sind die durch eine Untersuchung der DNA, RNA oder der Chromosomen gewonnenen Daten über genetische Eigenschaften eines Menschen. Genetische Daten sind wie Gesundheitsdaten zu behandeln.“***

bb) Biometrische Rechnungsgrundlagen

Der Begriff der biometrischen Daten muss klar auf „biometrische Erkennungsdaten“ begrenzt werden.

In der Versicherungsmedizin spielen sogenannte „biometrische Rechnungsgrundlagen“ eine Rolle, d. h. physische oder physiologische Merkmale werden in die versicherungsmathematischen Berechnungen einbezogen. Dies dürfte in Art. 4 Abs. 11 hier nicht gemeint sein. Es könnte jedoch zu Verwechslungen mit den gemeinten biometrische Erkennungsdaten kommen.

Vorschlag der deutschen Versicherungswirtschaft:

> ***In Art. 4 Abs. 11 sollte der Begriff „biometrische Erkennungsdaten“ verwendet werden.***

2. Tarifeinstufung und die Risikoeinschätzung in der Versicherungswirtschaft

a) Abgrenzung von der Profilbildung

Tarifierung und Risikoeinschätzung in der Versicherungswirtschaft müssen klar vom Begriff der Profilbildung in Art. 20 ausgenommen werden.

Hintergrund:

Es entspricht der Natur von Versicherungsverträgen, dass nach bestimmten Kriterien Risikogemeinschaften gebildet werden müssen. Dies geschieht in der Regel aufgrund der statistischen Auswertung bekannter Schadensfälle. Diese werden nach gemeinsamen Merkmalen zusammengefasst und lassen so den statistisch wahrscheinlichen Schadenverlauf der Merkmalsgruppe erkennen. Ein Beispiel dafür sind die in der Versicherungswirtschaft verwendeten Sterbetafeln. Die Wahrscheinlichkeit des Eintritts eines Versicherungsfalls und dessen Ausmaß werden im Einzelfall durch eine Risikoprüfung auf Grundlage der Angaben des Versicherungsnehmers mithilfe der Unternehmensstatistiken sowie weiterer bekannter Wahrscheinlichkeiten, wie medizinischer Erfahrungswerte, bewertet. Der Preis für den Versicherungsschutz wird dann entsprechend der Einordnung festgelegt.

Beispiele:

- In der Elementarschadenversicherung können Häuser, die in einem in regelmäßigen Abständen von Überschwemmungen betroffenen Ort liegen, nicht zu gleichen Konditionen versichert werden wie Häuser, die in einem Ort fernab von Gewässern liegen.
- Ebenso unterscheidet sich die Bemessung eines Beitrags danach, ob ein zu versicherndes Haus ein leicht brennbares Reetdach oder ein feuerfestes Schindeldach hat.
- Ein Hobbypilot kann nicht zu gleichen Bedingungen versichert werden, wie jemand, der kein gefährliches Hobby hat.
- Ein Mensch, der ein schweres Rückenleiden hat, kann in der Berufsunfähigkeitsversicherung nur zu ungünstigeren Bedingungen versichert werden, weil mit höherer Wahrscheinlichkeit Kosten auf die Versichertengemeinschaft zukommen.

Die Datenverarbeitung in der Versicherungswirtschaft wird ausführlich in der Empfehlung des Ministerkomitees des Europarates Rec (2002) 9 an die Mitgliedstaaten über den Schutz von zu Versicherungszwecken erhobenen und verarbeiteten personenbezogenen Daten geregelt. Hier werden auch „aktuarische Aktivitäten“ und damit auch die für die Versicherungswirtschaft wesensnotwendige Tarifierung erlaubt (Empfehlungen 4.4. k). Das Gleiche gilt für die Vorbereitung und den Abschluss der Versicherung, also Tarifeinstufung und Prämienbemessung (Empfehlungen 4.4. a).

Eine ordnungsgemäße Geschäftsorganisation eines Versicherers setzt nach Art. 44 der Solvency II-Rahmenrichtlinie (RL 2009/138/EG) ein angemessenes Risikomanagement voraus. Hierzu gehören auch die Risikoprüfung und -erkennung. Das Gesamtrisiko des Unternehmens ist aus der Aggregation der Einzelrisiken zu ermitteln. Im Rahmen der erforderlichen Risikosteuerung ist die Tarifierung und Risikoeinschätzung zwingend erforderlich.

Die Tarifeinstufung erfolgt in Massensparten teilweise auch automatisiert.
Dieser Trend wird sich in der Zukunft fortsetzen.

Verordnungsvorschlag der Kommission:

Der Vorschlag verbietet in Art. 20 grundsätzlich Profilbildungen aufgrund automatisierter Prozesse. Damit soll in erster Linie die Bildung von Verhaltensprofilen aufgrund von Aktivitäten im Internet verhindert werden. Die Bestimmung würde nach ihrem Wortlaut jedoch auch automatisierte Tarifeinstufungen und Risikoeinschätzungen in der Versicherungswirtschaft erfassen und damit die Arbeit der Versicherungswirtschaft im Kern gefährden. Tatsächlich handelt es sich jedoch um grundlegend andere Sachverhalte. Bei den versicherungstypischen Verfahrensweisen geht es gerade nicht darum, persönliche Präferenzen, Verhaltensweisen oder Einstellungen Einzelner zu analysieren oder vorherzusagen, sondern Gruppen mit gleichartigem Risikobild aufzustellen, um einem einzelnen Versicherten der Gruppe, den zufällig der Versicherungsfall trifft, aus der Summe der Beiträge Ersatz leisten zu können.

Eine **automatisierte Einschätzung aufgrund von Gesundheitsdaten**, z. B. in einer schnell abzuschließenden Reisekrankenversicherung, wäre nach **Art. 20 Abs. 3** generell verboten, selbst wenn das Ergebnis für die Kunden nur positiv ist. Eine solche Konsequenz ist vermutlich nicht gewollt und liegt nicht im Interesse der Kunden, denen die Kostenersparnis und der schnellere Policierungsprozess zugutekommen.

Die Regelung widerspricht auch Art. 9 Abs.1 der E-Commerce-Richtlinie vom 08.06.2000 (RL 2000/31/EG), in der es heißt:

> „Die Mitgliedstaaten stellen sicher, dass ihr Rechtssystem den Abschluss von Verträgen auf elektronischem Wege ermöglicht. Die Mitgliedstaaten stellen insbesondere sicher, dass ihre für den Vertragsabschluss geltenden Rechtsvorschriften weder Hindernisse für die Verwendung elektronischer Verträge bilden noch dazu führen, dass diese Verträge aufgrund des Umstandes, dass sie auf elektronischem Wege zustande gekommen sind, keine rechtliche Wirksamkeit oder Gültigkeit haben."

Die zukünftige Verordnung selbst stellt in diesem Punkt ein „Hindernis für die Verwendung elektronischer Verträge" dar, die durch die E-Commerce-Richtlinie gerade gefördert werden soll.

Position der deutschen Versicherungswirtschaft:

> ***Tarifierung und Risikoeinschätzung in der Versicherungswirtschaft müssen ausdrücklich vom Begriff der Profilbildung in Art. 20 ausgenommen werden.***

b) Zu weite Definition der Personenbeziehbarkeit von Daten

Die zu weite Definition personenbezogener Daten führt zu unverhältnismäßigen Einschränkungen bei der Verarbeitung wenig sensibler Sachdaten und pseudonymisierter Daten.

Hintergrund:

Zur Risikoeinschätzung nutzt die Versicherungswirtschaft auch wenig sensible Daten, die zunächst keiner Person zugeordnet sind.

Beispiel:

> In der Naturgefahrenversicherung ziehen Versicherer die frei zugänglichen Gefahrenkarten der öffentlichen Hand heran. So stellen etwa die deutschen Wasserwirtschaftsämter Informationen zu Überschwemmungsgebieten zur Verfügung, der Deutsche Wetterdienst hält Informationen zu Starkregen und Sturm vor. Hinzu kommen auflösungsbeschränkte Luftbilder des Bundesamtes für Kartografie und Geodäsie. Diese Daten sind zunächst nicht auf eine konkrete Person bezogen und von denjenigen, die sie weiterleiten, zumeist auch nicht auf eine bestimmte Person beziehbar.

Verordnungsvorschlag der Kommission:

Der Vorschlag geht in **Art. 4 Abs. 1 und 2** von einem **sehr weiten Begriff der Personenbeziehbarkeit** von Daten aus. Es genügt, dass irgendein Dritter – und nicht nur der für die Verarbeitung Verantwortliche – den Personenbezug herstellen könnte. Zum Begriff der personenbezogenen Daten wird damit die weiteste in der Literatur vertretende Rechtsmeinung zugrunde gelegt. Nicht einmal die Einschränkungen, die die Artikel 29-Datenschutzgruppe in ihrem Working Paper 136 (Stellungnahme 4/2007) zum Begriff „personenbezogene Daten“ vom 20. Juni 2007 gemacht hat, werden berücksichtigt.

Nach der weiten Definition läge in dem Beispielsfall bereits von Anfang an ein personenbeziehbares, also dem personenbezogenen gleichgestelltes Datum vor, weil die Möglichkeit besteht, dass jemand feststellt, dass ein Haus in einem Gebiet liegt, in dem Überschwemmungen häufig sind, und ein anderer dieses Haus einem Eigentümer zuordnen kann. Außerdem gelten für objektive, wenig sensible Sachdaten die gleichen Anforderungen wie für direkte Aussagen zu einer Person.

Da es nach der ausdrücklichen Regelung des Art. 4 Abs. 1 ausreicht, dass irgendjemand die Daten zu einer Kennnummer zuordnen kann, ist mit der Begriffsbestimmung außerdem auch jede Pseudonymisierung von Daten datenschutzrechtlich irrelevant.

Position der deutschen Versicherungswirtschaft:

Um ein **Ausufern des Begriffs der personenbezogenen Daten** und damit eine Verwässerung des Datenschutzrechts zu **vermeiden**, ist es erforderlich, die **Definition einzuschränken**. Es müssen **Privilegierungen für nicht unmittelbar personenbeziehbare Sachdaten sowie pseudonymisierte Daten** geschaffen werden.

Einschränkungen nur für vollständig anonymisierte Daten reichen nicht aus. Sofern für bestimmte Fälle diese Regelung zum Schutz des informationellen Selbstbestimmungsrechts nicht ausreicht, können diese gesondert geregelt werden.

Vorschlag der deutschen Versicherungswirtschaft:

Art. 4 Abs. 1 sollte wie folgt gefasst werden:

„'betroffene Person' eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt mit Mitteln bestimmt werden kann, die der für die Verarbeitung Verantwortliche ~~oder jede sonstige natürliche oder juristische Person~~ nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde, … "

3. Verhinderung von Versicherungsbetrug und Gewährleistung der Zuverlässigkeit von Versicherungsvermittlern

Den Auskunftssystemen der Versicherungswirtschaft zum Schutz vor Versicherungsbetrug und unzuverlässigen Versicherungsvermittlern darf die Rechtsgrundlage nicht entzogen werden.

Hintergrund:

Der deutschen Versicherungswirtschaft entstehen allein in der Schaden- und Unfallversicherung durch Versicherungsbetrug Verluste in einer geschätzten Höhe von vier Milliarden Euro pro Jahr.

> Eine Studie der Gesellschaft für Konsumforschung (GfK) aus dem Jahr 2011 ergab, dass ca. vier Prozent der befragten Haushalte offen zugaben, in den letzten fünf Jahren Versicherungsbetrug begangen zu haben. Weitere ca. sieben Prozent wissen von einem konkreten Versicherungsbetrug. Sonderuntersuchungen haben gezeigt, dass bis zu 40 % der Schäden an Smartphones, Flat-TV's und Laptops in Betrugsabsicht eingereicht wurden.

Diese Kosten verteuern den Versicherungsschutz für redliche Versicherungskunden erheblich. Die Versicherungswirtschaft ist daher im Interesse der Versicherten auf Maßnahmen der Betrugsbekämpfung angewiesen. Dem dient z. B. in Deutschland das **Hinweis- und Informationssystem (HIS)**, das erst im Jahr 2011 nach den Vorgaben der deutschen Datenschutzbehörden neu organisiert wurde. In diesem System werden bestimmte, auf ein erhöhtes Risiko hindeutende Daten aus den Versicherungsunternehmen gespeichert. Darüber hinaus kann es in klar definierten Fällen zu einem Datenaustausch zwischen betroffenen Versicherungsunternehmen kommen.

Auch die **Auskunftsstelle über den Versicherungs- und Bausparaußendienst (AVAD)** verarbeitet Informationen über Vermittler, um im Interesse der Verbraucher deren Zuverlässigkeit sicherzustellen. Satzungsmäßiger Zweck der AVAD ist es, zu erreichen, dass nur vertrauenswürdige Personen Versicherungs-, Bauspar- und sonstige Finanzdienstleistungsprodukte vermitteln. Ihre Tätigkeit dient der Umsetzung der Versicherungsvermittlerrichtlinie (Richtlinie 2002/92/EG des Europäischen Parlaments und des Rates vom 9. Dezember 2002 über Versicherungsvermittlung) in Deutschland. Die Identifizierung und Benennung unlauterer Vermittler ist notwendig, da keine laufende Kontrolle der Vermittler gewährleistet ist. Insbesondere für den Bereich der gebundenen Vermittler findet die Zuverlässigkeitsüberprüfung allein durch die Unternehmen statt. Hier ist die AVAD als Branchenauskunftei ein unverzichtbares Mittel der Überprüfung. Die AVAD ist daher sowohl von der Bundesanstalt für Finanzdienstleistungsaufsicht, also der deutschen Versicherungsaufsichtsbehörde als auch von den deutschen Datenschutzbehörden anerkannt.

In dem Betrugsbekämpfungssystem HIS werden auch **Verurteilungen wegen Versicherungsbetrugs** gespeichert und können von anderen Versicherern abgefragt werden. Die AVAD speichert ebenfalls **Strafurteile**, die sich auf die Zuverlässigkeit von Versicherungsvermittlern beziehen.

<u>Verordnungsvorschlag der Kommission:</u>

Für den Betrieb von Auskunfteien gibt es in dem Vorschlag für dieEU-Datenschutzgrundverordnung **keine klare gesetzliche Grundlage** mehr. Ob Art. 6 Abs. 1f. auch diese Fälle erfassen soll, ist unsicher, weil die Norm hinter Art. 7f) der RL 95/46/EG, der auch eine **Datenverarbeitung im Interesse Dritter** erfasst, zurückbleibt. Damit steht das Hinweis- und Informationssystem (HIS) der deutschen Versicherungswirtschaft, das der Bekämpfung von Versicherungsbetrug dient und auf Wunsch der Datenschutzbehörden gerade erst als Auskunftei ausgestaltet wurde, auf keiner sicheren Rechtsgrundlage mehr. Auch Datenübermittlungen an das System sowie an andere Unternehmen, die heute nach klar umschriebenen Kriterien erlaubt sind, werden zweifelhaft, weil Art. 6 Abs. 1f. des Verordnungsvorschlags keine Datenübermittlung im Interesse Dritter zulässt.

Entsprechendes gilt für die Auskunftsstelle über den Versicherungs- und Bausparaußendienst (AVAD).
Durch Art. 9 Abs. 1, 2 (j) wird die Verarbeitung von Daten über Strafurteile an eine rechtlich gerade in diesem Fall sehr unsichere Einwilligung oder ein spezielles nationales oder europäisches Gesetz geknüpft. Ein solches Gesetz liegt zumindest in Deutschland nicht vor.

Position der deutschen Versicherungswirtschaft:

Der Betrieb der genannten Systeme muss sichergestellt werden, indem eine Datenverarbeitung im Interesse Dritter zugelassen wird sowie eine Verarbeitung von Daten über Strafurteile bei erheblichem berechtigten Interesse unmittelbar aufgrund der Verordnung ermöglicht wird.

Vorschlag der deutschen Versicherungswirtschaft:

Art. 6 Abs. 1 f) Satz 1 sollte wie folgt gefasst werden:

> ***„Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.“***

Art. 9 Abs. 2 j) sollte wie folgt gefasst werden:

> ***„die Verarbeitung von Daten über Strafurteile oder damit zusammenhängende Sicherungsmaßregeln erfolgt entweder unter behördlicher Aufsicht oder aufgrund einer gesetzlichen oder rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt, oder zur Wahrnehmung eines wichtigen öffentlichen Interesses oder sonstigen erheblichen berechtigten Interesses, das die schutzwürdigen Interessen der Betroffenen deutlich überwiegt. Ein vollständiges Strafregister darf nur unter behördlicher Aufsicht geführt werden.“***

4. Betroffenenrechte

Umfangreiche Betroffenenrechte dürfen die Vertragsdurchführung und die Durchführung sinnvoller Geschäftsprozesse nicht gefährden.

Ein effektiver Datenschutz setzt voraus, dass die Betroffenen über die Verarbeitung ihrer Daten informiert sind. Jedoch gehen die Rechte, die den Betroffenen durch die Verordnung eingeräumt werden, weit über das aktuelle Datenschutzniveau aller Mitgliedstaaten hinaus. Sie übersteigen sogar den als besonders hoch geltenden deutschen Datenschutzstandard.

Für die Unternehmen bedeuten umfangreiche Benachrichtigungs- und Auskunftspflichten sowie die Rechte auf Vergessenwerden und auf Datenübertragbarkeit nicht nur erheblichen Bürokratieaufwand. Es besteht auch die Gefahr, dass notwendige und sinnvolle Geschäftsabläufe, die auch im Interesse der Kunden liegen, behindert oder sogar unmöglich gemacht werden. Es muss dabei darauf geachtet werden, dass Regelungen, die für soziale Online-Netzwerke passend sind, nicht 1:1 auf den Offline-Betrieb übertragen werden.

a) Recht auf Vergessenwerden und Löschung

In Art. 17 wird ein umfangreiches **Recht auf Vergessenwerden und Löschung** geregelt.

Art. 17 sieht in Absatz 1 zahlreiche Gründe vor, die zur Löschung der Daten führen müssen, u. a. auch den Widerruf einer Einwilligung (Art. 17 Abs. 1b) bzw. d). Da die Alternativen des Art. 17 Abs. 1 nebeneinanderstehen, gilt dies selbst während eines laufenden Vertrages. Jedoch darf es z. B. nicht möglich sein, dass ein Kunde dem Versicherer den Datenbestand ganz oder zum Teil entzieht und damit eine sachliche Leistungsprüfung unmöglich macht oder sich vorzeitig vom Vertrag löst.

Position der deutschen Versicherungswirtschaft:

Das Recht auf Vergessenwerden muss ausgeschlossen sein, wenn die Daten zur Durchführung eines Vertrages erforderlich sind.

Vorschlag der deutschen Versicherungswirtschaft:

In Art. 17 Abs. 3 sollte am Ende ein neuer Buchstabe e eingefügt werden (Buchstabe e wird Buchstabe f):

> ***„für die Durchführung eines Vertrages oder die Erfüllung gesetzlicher Ansprüche.“***

b) Sperrung statt Löschung

Die heutigen technischen Systeme ermöglichen in aller Regel keine vollständige Löschung der Daten. So lassen sich etwa aus auf Speicherplatten fotografisch gesicherten Daten keine Teildateien entfernen. Derartige Speichermethoden werden z. B. in Bereichen verwendet, in denen eingescannte Daten nach Vernichtung der Dokumente unveränderbar zur Verfügung stehen müssen. Die Verpflichtung zur vollständigen Löschung wird damit unerfüllbar. Es kann lediglich der Zugriff unmöglich gemacht werden.

Position der deutschen Versicherungswirtschaft:

Für diesen Fall, dass eine Löschung aus technischen Gründen nicht möglich ist, muss eine Sperrung der Daten ausreichen, wie es z. B. in Deutschland in § 35 Abs. 3 Nr. 3 BDSG vorgesehen ist.

Vorschlag der deutschen Versicherungswirtschaft:

In Art. 17 Abs. 4 wird am Ende eingefügt:

> ***„e) eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.“***

c) Recht auf Datenübertragbarkeit

Ein Recht auf Datenübertragbarkeit nach Art. 18 kann wohl dann sinnvoll angewendet werden, wenn eine Person **eigene Inhalte** in das **Internet** stellt, wie z. B. Fotos oder Texte in sozialen Online-Netzwerken. Es ist auch dann nachvollziehbar, wenn Personen eigene Dateien einem Cloud-Anbieter zur Speicherung überlassen. Bei diesen Internet-Anwendungen muss es grundsätzlich möglich sein, die Inhalte wieder zu entfernen oder einem anderen Anbieter zu übertragen. Jedoch geht der Anwendungsbereich des Art. 18 weit über diese Fallgruppen hinaus.

In der Versicherungswirtschaft werden die Daten gesichert zu Zwecken der Vertragsdurchführung oder Abwicklung von Ansprüchen verarbeitet. Da jedoch auch **strukturierte Formate** verwendet werden, müssten Versicherungsunternehmen nach **Art. 18 Abs. 1** Kopien der von ihnen verarbeiteten Daten in einem für die jeweilige Person weiterverwendbaren strukturierten elektronischen Format zur Verfügung stellen. Da die Datenverarbeitungssysteme für völlig andere Abläufe programmiert sind, wäre das nur mit erheblichem technischen und finanziellen Aufwand möglich und ginge über den Unternehmenszweck weit hinaus.

Noch weiter geht **Art. 18 Abs. 2**, der immer eingreift, wenn eine Person ihre Daten zur Verfügung gestellt hat und die Verarbeitung auf einer Einwilligung oder einem Vertrag basiert. Damit fielen z. B. die meisten Kundendaten darunter, die Versicherer verarbeiten. Eine **Überführung der Daten in andere Systeme** ist nicht nur technisch aufwendig. Sie würde auch für den Kunden keinen Nutzen generieren, da beim neuen Versicherer andere Tarife gelten. Zudem wären aus den Datensätzen Tarifstrukturen und damit Geschäftsgeheimnisse erkennbar, sodass auch erhebliche wettbewerbsrechtliche Bedenken bestehen.

Position der deutschen Versicherungswirtschaft:

In der Versicherungswirtschaft, die die Daten zur Durchführung von Verträgen oder zur Erfüllung von Ansprüchen gesichert verarbeitet, ergibt das Recht auf Datenübertragbarkeit keinen Sinn.

Vorschlag der deutschen Versicherungswirtschaft:

> ***Art. 18 Abs. 1 und 2 müssen auf die Fälle begrenzt werden, in denen die Betroffenen eigene Inhalte in das Internet eingestellt haben.***

d) Informations- und Auskunftsrechte

Transparenz ist ein wichtiges Element des Datenschutzes. Die Betroffenen sollten daher wissen, wer ihre Daten verarbeitet und im Detail Auskunft erhalten können. Zu umfangreich und praktisch kaum erfüllbar sind die **Informationspflichten** aus Art. 14 und die **Auskunftspflichten** aus Art. 15. Die Informationspflichten nach Art. 14 haben bereits eine Detailtiefe, die für viele Kunden nicht von Interesse sein dürfte. Sie können durch delegierte Rechtsakte noch weiter ausgestaltet werden. Damit gehen sie selbst über das scharfe deutsche Recht deutlich hinaus. Auskunftsrechte können in Branchen, die wie die Versicherungswirtschaft umfangreiche Daten verarbeiten, uferlos werden, wenn sie nicht spezifiziert werden. Sie müssen dort an ihrer Grenzen stoßen, wo Tatsachen geheimhaltungsbedürftig sind.

Position der deutschen Versicherungswirtschaft:

Den Betroffenen sollten mit Art. 14 nicht umfangreiche Informationen aufgedrängt werden, sondern sie sollten die Informationen erhalten, die sie benötigen, um ihr Auskunftsrecht wahrzunehmen. Auskunftswünsche sollten vom Betroffenen spezifiziert werden, um zielgerichtet antworten zu können und unnötigen Rechercheaufwand zu vermeiden.

Ein Vorbild können die Regelungen im deutschen Recht, §§ 33 und 34 BDSG einschließlich der dort genannten Ausnahmen sein.

5. Vermeidung bürokratischer Belastungen

Im Hinblick auf den ohnehin schon hohen Datenschutzstandard sollte die Regelung der Anforderungen an Datenschutz und Datensicherheit mit Augenmaß erfolgen und unnötige bürokratische Belastungen vermeiden.

Entgegen dem erklärten Ziel der Kommission, Bürokratie abzubauen, bringt die Verordnung erhebliche neue bürokratische Belastungen mit sich. Durch den gesamten Verordnungsvorschlag ziehen sich Anforderungen an die Unternehmen, die ganz erheblichen Verwaltungsaufwand zur Folge haben. Nur bespielhaft genannt seien die detaillierten und umfangreichen Vorschriften zur Erstellung und zum Nachweis von Datenschutzstrategien (Art. 22), zur Implementierung und zum Einsatz datenschutzfreundlicher Technik (Art. 23), zur Dokumentation der Verarbeitungsvorgänge (Art. 28), zur Gewährleistung der Datensicherheit (Art. 30) und zur Zusammenarbeit mit der Aufsichtsbehörde (Art. 29, 34). Diese ohnehin schon umfangreichen Pflichten können in aller Regel von der Kommission noch durch delegierte Rechtsakte weiter konkretisiert oder durch Durchführungsbestimmungen formalisiert werden.

Nachfolgend wird nur auf die besonders einschneidenden Pflichten eingegangen.

a) Datenschutzfolgeabschätzung nach Art. 33

Angesichts der Vielzahl von Verpflichtungen, die bereits bestehen, ist das zusätzliche Erfordernis einer Datenschutzfolgeabschätzung nach Art. 33 nicht nachvollziehbar.

Bereits der **Anwendungsbereich der Norm ist nicht eindeutig**. So stellt sich die Frage, wann ein Verarbeitungsvorgang „konkrete Risiken“ für die Rechte und Freiheiten betroffener Personen“ birgt. Das Regelbeispiel des Art. 33 Abs. 2a) dürfte so zu verstehen sein, dass zahlreiche Datenverarbeitungen in der Versicherungswirtschaft, wie z. B. die Einstufung in einen Tarif, eine Datenschutzfolgeabschätzung erfordern. Nach Art. 33 Abs. 2 b) scheint die gesamte Datenverarbeitung in der Personenversicherung der Datenschutzfolgeabschätzung zu bedürfen, wenn Gesundheitsdaten von Einzelpersonen erfasst sind. Da die Aufsichtsbehörde für weitere Verarbeitungsvorgänge eine Folgenabschätzung verlangen kann (Art. 33 Abs. 2e), Art. 34 Abs. 2b)), ist der Anwendungsbereich der Regelung unabsehbar. Auch ist nicht klar, welchen **Inhalt und Umfang** die Folgenabschätzung haben soll. Die nähere Bestimmung ist nach Art. 33 Abs. 6 der Kommission überlassen.

Besonders belastend ist die Regelung des **Art. 33 Abs. 4**. Danach muss die **Einschätzung der Betroffenen oder ihrer Repräsentanten** eingeholt werden. Dies führt nicht nur zu erheblichem Bürokratieaufwand, sondern **gefährdet Geschäftsgeheimnisse**. Schließlich ist anzunehmen, dass auf diesem Weg auch der Marktgegenseite geplante Verfahren bekannt werden. Art. 33 in der vorgeschlagenen Fassung stellt damit einen unverhältnismäßigen Eingriff in die unternehmerische Freiheit dar.

Position der deutschen Versicherungswirtschaft:

Da die Auswirkungen einer Datenverarbeitung für die Betroffenen ohnehin im Rahmen der anderen Anforderungen, wie z. B. des Art. 23, beachtet werden müssen, ist Art. 33 entbehrlich.

Vorschlag der deutschen Versicherungswirtschaft:

Art. 33 wird gestrichen.

b) Reaktion auf Datenpannen (Art. 31 und 32)

Die Verpflichtung zur **Meldung von Datenpannen** wird sogar im Vergleich zu dem sehr weitgehenden deutschen Recht sehr strikt ausgestaltet. Nach Art. 4 Abs. 9, 31, 32 genügt bereits jede Zerstörung, jeder Verlust, jede Veränderung oder jeder unberechtigte Zugriff auf personenbezogene Daten. Es kommt weder darauf an, ob die Daten ihrer Art nach besonders schutzwürdig sind noch auf die Schwere und Tragweite des Vorfalls für die Betroffenen. Ein so **weit gefasster Anwendungsbereich** lässt eine **Meldeflut** bei den Aufsichtsbehörden und eine Abstumpfung der immer wieder auch in nichtigen Fällen benachrichtigten Betroffenen befürchten.

Position der deutschen Versicherungswirtschaft:

Art. 31 und 32 sollten so eingeschränkt werden, dass

- ***nur besonders schutzwürdige Daten erfasst sind,***
- ***nur die unrechtmäßige Übermittlung oder sonstige unrechtmäßige Kenntniserlangung erfasst sind und***
- ***schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen müssen.***

Als Vorbild kann der im Jahr 2009 in das deutsche Bundesdatenschutzgesetz eingefügte § 42a BDSG dienen.

6. One stop-shop

Künftig ist nach Art. 51 Abs. 2 die Aufsichtsbehörde am Hauptsitz eines Unternehmens auch für dessen Zweigniederlassungen zuständig. Für europaweit tätige Unternehmen bedeutet es eine erhebliche Erleichterung, dass Meldungen, Genehmigungs- und Dokumentationserfordernisse nur noch einmal zentral bei der zuständigen Datenschutzbehörde erfolgen müssen.

Allerdings ist dieser Vorteil nur begrenzt, weil die meisten Konzerne so organisiert sind, dass sie rechtlich selbständige Tochtergesellschaften haben. Jede Tochtergesellschaft ist grundsätzlich eine eigene verantwortliche Stelle im Sinne der Verordnung. Für sie ist daher jeweils die Aufsichtsbehörde in dem Mitgliedstaat zuständig, in dem die Tochtergesellschaft ihren Sitz hat. Ob Art. 24 so weit ausgelegt werden kann, dass eine Zuständigkeit nur der Aufsichtsbehörde der Muttergesellschaft begründet werden kann, ist zweifelhaft.

Meldepflichten, Genehmigungs-/ Dokumentationserfordernisse etc. fallen also jeweils pro Tochtergesellschaft und damit mehrfach an. Binding Corporate Rules nach Art. 43 des Verordnungsvorschlags müssen nicht nur von der Konzernmutter zur Genehmigung bei der zuständigen Aufsichtsbehörde eingereicht werden, sondern auch von Tochtergesellschaften in anderen EU-Mitgliedstaaten bei den für sie zuständigen Behörden. Damit bleibt es bei erheblichem Bürokratieaufwand.

Vorschlag der deutschen Versicherungswirtschaft:

> ***Die zentrale Zuständigkeit der Aufsichtsbehörde nach Art. 51 Abs. 2 sollte nicht nur Niederlassungen, sondern auch Konzerntöchter entsprechend der Definition in Art. 4 Abs. 16 des Verordnungsentwurfs erfassen.***

7. Kollektive Rechtsdurchsetzung

Über Art. 76 Abs. 1 i. V. m. Art. 75 werden Datenschutzverbände auch zu **Sammelklagen** berechtigt. Es ist jedoch kein Rechtsdurchsetzungsdefizit erkennbar, das derartige Klagen rechtfertigt. Das gilt im Datenschutzrecht noch mehr als im Verbraucherschutzrecht. Zur Ahndung möglicher Datenschutzverstöße gibt es hier nämlich – anders als z. B. bei der Überprüfung von AGB – spezielle Datenschutzaufsichtsbehörden, die nach der Verordnung umfangreiche Eingriffsbefugnisse haben. Jeder Betroffene kann sich form- und kostenlos an die Behörden wenden. Nach dem Verordnungsvorschlag soll den Datenschutzbehörden in Art. 76 Abs. 2 sogar eine Klagebefugnis verliehen werden.

Vorschlag der deutschen Versicherungswirtschaft:

> ***Art. 76 Abs. 1 sollte gestrichen werden.***

8. Sanktionen

Gerade angesichts der oben geschilderten umfangreichen Anforderungen und der hohen Rechtsunsicherheiten escheinen die umfangreichen Sank-

tionen in Art. 79 sehr einschneidend. Hier sollten aber zunächst die Vorschriften angepasst werden, deren Verletzung sanktioniert wird. Auch für große Unternehmen sollte die Möglichkeit der Verwarnung bei ersten unbeabsichtigten Verstößen (Art. 79 Abs. 3) eröffnet werden.

Vorschlag der deutschen Versicherungswirtschaft:

Art. 79 Abs. 3 sollte wie folgt gefasst werden:

> ***„Handelt es sich um einen ersten, unabsichtlichen Verstoß gegen diese Verordnung, kann anstatt einer Sanktion eine schriftliche Verwarnung erfolgen."***

9. Delegierte Rechtsakte und Durchführungsakte

Eine abschließende Einschätzung der Auswirkungen des Verordnungsvorschlags gestaltet sich schwierig, weil an zahlreichen Stellen Ermächtigungen der Kommission zu delegierten Rechtsakten nach Art. 86 bzw. zu Durchführungsrechtsakten nach dem in Art. 87 vorgegebenen Verfahren in dem Vorschlag enthalten sind. Während Durchführungsrechtsakte in einzelnen Bereichen aufgrund erforderlicher Anpassungen an technische Entwicklungen gerechtfertigt sein mögen, erscheinen die umfangreichen Gestaltungsbefugnisse der Kommission in der Gesamtschau als zu weitgehend, da sie eine erhebliche Rechtsunsicherheit für die datenverarbeitende Wirtschaft bedeuten. Nach Art. 290 AEUV kann der Kommission die Befugnis übertragen werden, Rechtsakte ohne Gesetzescharakter mit allgemeiner Geltung zur Ergänzung oder Änderung bestimmter nicht wesentlicher Vorschriften des betreffenden Gesetzgebungsaktes zu erlassen. Es kann nicht angenommen werden, dass die Vielzahl der Vorschriften, die geändert werden können, nicht wesentlich sind. Außerdem müssen bereits die Regelungen der zukünftigen Verordnung hinreichend bestimmt sein. Gerade angesichts der massiven Sanktionsvorschriften muss für die Verantwortlichen von vornherein klar erkennbar sein, wie weit ihre Pflichten gehen.

Position der deutschen Versicherungswirtschaft:

Anstelle von delegierten Rechtsakten sollte das Datenschutzrecht in den einzelnen Sektoren durch Selbstregulierungsmaßnahmen konkretisiert werden. **Die deutsche Versicherungswirtschaft geht diesen Weg gemeinsam mit den deutschen Datenschutzbehörden bereits nach dem aktuellen deutschen Datenschutzrecht (siehe oben Vorbemerkung).** Der Verordnungsvorschlag wählt hierzu in Art. 38 einen richtigen Ansatz. Jedoch sollten die Anforderungen an den Inhalt weniger starr festgelegt werden, um eine breite Akzeptanz und Praktikabilität zu sichern.

Berlin, den 30.03.2012