

Positionspapier

EU-Datenschutz-Grundverordnung

„Die Gesamtbalance fehlt noch“

Münchener Rückversicherungs-
Gesellschaft
Datenschutzbeauftragter
14.09.2012

1 Position der Munich Re Gruppe

Munich Re begrüßt die Zielsetzung, das Datenschutzrecht in Europa zu vereinheitlichen und Hemmnisse für grenzüberschreitend tätige Unternehmen beim internationalen Datenaustausch abzubauen.

Im Hinblick auf (rück-)versicherungsspezifische Geschäftsabläufe enthält der Vorschlag der Datenschutz-Grundverordnung jedoch noch erhebliche rechtliche Unsicherheiten sowie Bestimmungen, die die Bereitstellung von Versicherungsschutz erheblich erschweren, verteuern und in Teilen sogar gefährden würden. Ziel der Verordnung sollte es sein, sowohl in dieser Hinsicht wie auch bei den den Unternehmen auferlegten bürokratischen Pflichten einen angemesseneren Ausgleich zwischen den Interessen der Betroffenen und der Unternehmen zu schaffen.

Aus den bzw. neben den von den maßgeblichen Verbänden und Interessenvertretungen bereits vorgebrachten Punkten, möchten wir vor allem auf folgende Aspekte hinweisen.

1.1 Es bedarf einer eindeutigen Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten in der Lebens-, Kranken-, Unfall- und Haftpflichtversicherung einschließlich der Rückversicherung. Gesundheitsdaten sind u.a. eine zwingende Voraussetzung für eine risikoadäquate Prämienfestsetzung. Bedingt durch den medizinischen Fortschritt (verbesserte Diagnostik und Therapieverfahren) können in diesem Zusammenhang auch relevante genetische Informationen (z.B. im Rahmen der Arzthaftpflichtversicherung) umfasst sein. Die vom Verordnungsvorschlag zu genetischen Daten verwendete Definition ist zu weitgehend (z. B. ist auch das für jedermann sichtbare Geschlecht erfasst) und muss noch eingegrenzt werden. Genetische Informationen sind naturgemäß Bestandteil von Gesundheitsdaten, da nahezu jede Erkrankung einen genetischen Hintergrund aufweist. Dieser Umstand sollte berücksichtigt werden.

Der Rückversicherer muss auch künftig die für seine Geschäftstätigkeit erforderlichen personenbezogenen Daten einschließlich der Gesundheits- und genetischen Daten vom Erstversicherer erhalten und verarbeiten können. In einigen

Fällen kann es das versicherte Risiko zudem erfordern, dass der Rückversicherer sich weiterer Rückversicherer (Retrozessionäre) bedient und dazu ebenfalls im erforderlichen Umfang personenbezogene Daten weitergeben können muss.

1.2 Die auf das Internet zugeschnittenen Bestimmungen zur **Profilbildung** (Art. 20) dürfen die Tarifeinstufung und Risikoeinschätzung als Kernbestandteile des Versicherungsgeschäfts nicht einschränken.

1.3 Die Möglichkeit der **Pseudonymisierung** personenbezogener Daten muss in der Verordnung noch ergänzt werden, um auch künftig die für das Versicherungsgeschäft unabdingbaren (klinischen) Studien auswerten oder als Rückversicherer Portfolioanalysen über den Versicherungsbestand bei Erstversicherungsunternehmen durchführen zu können. Es muss klargestellt sein, dass der Empfänger, der pseudonymisierte Daten erhält, diese aber nicht bestimmten Personen zuordnen kann, die Daten anonymisiert verarbeitet und insoweit nicht den Regelungen der Verordnung unterliegt.

1.4 Die besondere Situation von **Unternehmensgruppen** (Konzerne) muss sich in einer Rechtsgrundlage für einen erleichterten Transfer von Daten zwischen den einzelnen Gesellschaften niederschlagen, um Aufgaben - unter Beibehaltung der Zweckbindung der Daten - innerhalb eines Konzerns sinnvoll aufzuteilen und auch zu zentralisieren.

1.5 Es muss klargestellt sein, dass sich der **territoriale Anwendungsbereich des europäischen Datenschutzrechts** (Art. 3 Abs. 1) nicht auf in Drittstaaten niedergelassene verantwortliche Stellen erstreckt, die personenbezogene Daten ausschließlich betreffend Nicht-EU-Bürger durch einen in der EU niedergelassenen Auftragsverarbeiter (z.B. ein Konzernrechenzentrum) verarbeiten lassen. Materielle Zulässigkeitstatbestände für die Datenerhebung/-verarbeitung/-nutzung oder formelle Anforderungen (z.B. Bestellung eines Datenschutzbeauftragten) dürfen nicht über den Auftragsverarbeiter auch auf den Auftraggeber im Drittstaat durchschlagen.

1.6 Der Ansatz des „one-stop-shops“ (Art. 51) für die **Zuständigkeit der Aufsichtsbehörde** wird begrüßt, sollte aber neben Niederlassungen auch Tochtergesellschaften umfassen.

2 Argumente

Die Kenntnis personenbezogener Angaben des Versicherungsnehmers, Versicherten oder Geschädigten ist in der Versicherungswirtschaft zur Risikoprüfung und Leistungsabwicklung unabdingbar. In vielen Bereichen gilt das auch für Rückversicherer: anonymisierte oder pseudonymisierte Angaben reichen dort regelmäßig nicht aus. Ohne eine verlässliche, auch und vor allem personenbezogene Information kann sich ein Rückversicherer sehr häufig nicht auf die Rückversicherung eines Risikos einlassen. Das ist insbesondere dann der Fall, wenn die Versicherungssumme besonders hoch ist oder es sich um ein schwierig einzustufendes Risiko handelt. Auch muss der Rückversicherer erkennen können, wenn ihm das gleiche Risiko – bei Lebensversicherungen z.B. der glei-

che Versicherungsnehmer – von verschiedenen Erstversicherern vorgelegt wird, um zu überprüfen, ob und in welcher Höhe er sich an dem Risiko beteiligen kann. Darüber hinaus ist es möglich, dass der Rückversicherer den Erstversicherer aufgrund seiner besonderen Sachkunde bei der Risiko- oder Leistungsprüfung sowie bei der Bewertung von Verfahrensabläufen unterstützt. Haben Rückversicherer die Absicherung des Risikos übernommen, müssen sie zudem kontrollieren können, ob der Erstversicherer das Risiko bzw. einen Leistungsfall richtig eingeschätzt und Prämienzahlungen bzw. Leistungsfälle zutreffend abgerechnet werden. Dazu bedarf es jeweils einer personenbezogenen Zuordnung.

2.1 Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten

Versicherungsschutz steht den Betroffenen nur dann zur Verfügung, wenn der (Rück-) Versicherer die zu versichernden Risiken – auch im Einklang mit versicherungsaufsichtsrechtlichen Bestimmungen – im erforderlichen Umfang prüfen kann. In der Kranken-, Lebens-, Unfall- wie auch Haftpflichtversicherung sind dazu Gesundheitsdaten regelmäßig die notwendige Grundlage zum Abschluss, zur Durchführung und Erfüllung der Versicherungsverträge. Dies gilt im vorgenannten Rahmen auch bei der betreffenden Rückversicherung.

Beispiel:

- 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. Übernimmt der Rückversicherer den überwiegenden Anteil an einer von dem Erstversicherer gezeichneten Versicherung, obliegt ihm naturgemäß auch die Hauptlast der Risiko- bzw. Leistungsprüfung.

Die Abwicklung von Versicherungsfällen mit Personenschäden ist ebenfalls nur möglich, wenn dem (Rück-) Versicherer die dazu notwendigen Daten einschließlich der Gesundheitsdaten verarbeiten kann.

In einigen Fällen erstrecken sich die Gesundheitsdaten dabei auch auf etwaig erforderliche genetische Daten. Deutsche Versicherer verlangen zwar weder vor noch nach Abschluss eines Versicherungsvertrages die Durchführung genetischer Untersuchungen. Auf die Ergebnisse vorhandener genetischer Untersuchungen muss im Rahmen des gesetzlich Zulässigen aber bei Abschluss von Verträgen mit sehr hohen Beitragssummen zurückgegriffen werden können. Möglich bleiben muss auch 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 zunehmend wichtiger werdende Rolle. Diagnostische und prognostische Zuordnungen vieler Krebserkrankungen (z.B. Brustkrebs, Leukämien, Lymphome) erfolgen zunehmend auf der Basis genetischer Informationen. Aber auch die Auswahl an Behandlungen wird oftmals durch genetische Informationen mitbestimmt. Die Versicherungswirtschaft benötigt diese Untersuchungsergebnisse für die Risikoprüfung und Leistungsbear-

beutung in der Personen(rück-)versicherung. Die Nutzung der Daten für die Prüfung einer bestehenden, diagnostizierten Erkrankung darf nicht davon abhängen, welche Untersuchungsmethode ein Arzt zugrunde legt.

Unter der geltenden Datenschutzrichtlinie 95/46/EG kann sich die Weitergabe personenbezogener Versicherungsnehmerdaten vom Erstversicherer an den Rückversicherer derzeit auf berechnigte Interessen im Sinne des Art. 7 f. stützen. Bei der Weitergabe besonderer Arten personenbezogener Daten – hier von Gesundheitsdaten – müssen die betroffenen Versicherungsnehmer jedoch zusätzlich zum Versicherungsvertrag noch eine gesonderte Einwilligungserklärung abgeben (Art. 8 Abs. 2 a Richtlinie 95/46/EG), damit der Versicherer die notwendigen Gesundheitsdaten verarbeiten und auch an Rückversicherer im erforderlichen Umfang weitergeben kann. Ohne eine solche Einwilligung wird in den meisten Fällen ein Versicherungsschutz nicht gewährt werden können, so dass schon heute fraglich sein könnte, ob die Einwilligung tatsächlich ohne jeden Zwang abgegeben wird. Durch die im Verordnungsentwurf vorgesehenen Neuregelungen – vor allem in Art. 7 Abs. 4 des Vorschlags – wird eine Einwilligung für einzelne, vor allem existenzabsichernde Versicherungsbereiche künftig generell ausgeschlossen, sofern zwischen dem Versicherer einerseits und dem Versicherungsnehmer bzw. dem Versicherten ein „erhebliches Ungleichgewicht“ anzunehmen ist. Dies würde u.a. im Bereich der Lebensversicherung die Geschäftsabwicklung unmöglich machen.

Als weltweit tätiger Rückversicherer zählen zudem zu unseren Kunden auch Erstversicherungsunternehmen aus Drittstaaten außerhalb des Geltungsbezugs der vorgeschlagenen Verordnung. Diese holen bei ihren Versicherungsnehmern regelmäßig keine den Anforderungen des EU-Datenschutzrecht genügende Einwilligungen zur Datenweitergabe an Rückversicherer ein. Die Verarbeitung der erforderlichen Gesundheitsdaten beim Rückversicherer kann in solchen Fällen lediglich auf ein Erfordernis zur Begründung, Geltendmachung oder Abwehr von Rechtsansprüchen (Art. 9 Abs. 2 f der vorgeschlagenen Verordnung) stützen. Eine klarere und damit für den Rückversicherer rechtssichere Verarbeitungsgrundlage in der Verordnung wäre wünschenswert.

2.2 Profilbildung

Es entspricht der Natur von Versicherungsverträgen, dass nach bestimmten Kriterien Risikogemeinschaften gebildet werden müssen. Dies geschieht in der Regel aufgrund von statistischen Auswertungen. 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 Versicherungsfalles wird fast immer durch eine individuelle Risikoprüfung auf Grundlage der Angaben des Versicherungsnehmers mithilfe von Einschätzungsgrundsätzen (Manualen), Unternehmensstatistiken sowie weiterer bekannter Wahrscheinlichkeiten, wie medizinischer Erfahrungswissen, bewertet und quantifiziert. Der Preis für den Versicherungsschutz wird dann entsprechend dieser langzeitprognostischen Einordnung festgelegt.

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 „aktuari-sche Aktivitäten“ und damit auch die für die Versicherungswirtschaft wesens-notwendige 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 Risi-komanagement 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 aber auch bei individuellen Verträgen mit einfachen Risiken (z.B. Übergewicht) zunehmend auch automatisiert. Dieser Trend wird sich in der Zukunft fortsetzen.

Es muss daher klargestellt sein, dass Tarifierung und Risikoeinschätzung in der Versicherungswirtschaft ausdrücklich vom Begriff der Profilbildung in Art. 20 ausgenommen sind.

2.3 Pseudonymisierung

Um – wie bereits erwähnt - die Wahrscheinlichkeit des Eintritts eines Versiche-rungsfalls und dessen Ausmaß sinnvoll einzuschätzen, benötigt der (Rück-)Ver-sicherer dem Versicherungsantrag vergleichbare Erfahrungswerte und statisti-sche Informationen. Aussagekräftige Statistiken erfordern wiederum eine mög-lichst breite Datenbasis. Eine wesentliche Grundlagen dafür bilden pseudonymi-sierte Angaben zu Schadenfällen oder Krankheitsverläufen (z.B. bei klinischen Studien mit den Endpunkten Tod oder Pflegefall oder bleibende Behinderung). Anonymisierte Daten reichen dazu nicht, da zeitlich nachfolgende Entwicklungen nicht mehr zuordenbar wären und Erkenntnisse (z.B. zu Krankheitsverläufen) verloren gingen.

Der sehr weite Begriff der Personenbeziehbarkeit von Daten in Art. 4 Abs. 1 und 2 des Vorschlags behandelt pseudonymisierte Daten – soweit erkennbar – künftig auch bei einem Empfänger, der die Angaben selbst nicht auf bestimmte Personen rückführen kann, als personenbezogen. Es genügt, dass irgendein Dritter – und nicht nur der für die Verarbeitung Verantwortliche – den Zuord-nungsschlüssel besitzt und einen Personenbezug herstellen könnte. Dies selbst dann, wenn ein Zugriff des für die Verarbeitung Verantwortlichen tatsächlich ausgeschlossen ist. Dies kann aber dazu führen, dass Rückversicherern der Zugang zu extern erhobenen Daten wie z.B. klinischen Studien verschlossen bliebe, die als wesentliche Grundlage für statistische Belegbarkeit der Risikoer-schwerungen von Einschätzungsgrundsätzen dienen. Gerade die statistische Belegbarkeit wird aber im Richtlinienvorschlag der EU Kommission zur Anwen-

derung des Grundsatzes der Gleichbehandlung ungeachtet der Religion oder der Weltanschauung, einer Behinderung, des Alters oder der sexuellen Ausrichtung (KOM(2008) 426 explizit gefordert (Artikel 2 Absatz 5).

Die Möglichkeit der Pseudonymisierung muss in der künftigen Verordnung vorgesehen werden und es muss klargestellt sein, dass der Empfänger, der pseudonymisierte Daten erhält, diese aber nicht bestimmten Personen zuordnen kann, die Daten anonymisiert verarbeiten darf.

2.4 Unternehmensgruppen

Der Verordnungsentwurf definiert zwar den Begriff der Unternehmensgruppe, macht von dieser Definition aber kaum Gebrauch. Es wird lediglich die Möglichkeit eingeräumt, einen Konzerndatenschutzbeauftragten zu bestellen (Art. 35 Abs. 2), und bei der Auftragsverarbeitung (Art. 26 Abs. 5) kann die Kommission in delegierten Rechtsakten Bedingungen festlegen, um die Verarbeitung personenbezogener Daten in Unternehmensgruppen zu Kontroll- und Berichterstattungszwecken zu vereinfachen.

Dies reicht als Grundlage für einen angemessenen Datenaustausch innerhalb solcher Unternehmensgruppen nicht aus. Um Synergien zu erzielen, werden innerhalb von (Rück-)Versicherungsgruppen Serviceaufgaben delegiert und zentralisiert. Das gilt nicht nur für die EDV in einem Konzernrechenzentrum, sondern z.B. auch für die Personalverwaltung/-planung, Risikoeinschätzung oder Schadenabwicklung. Die Zwecke der Datenverarbeitung werden dadurch nicht geändert, die Zweckbindung bliebe also sichergestellt. Die (Erst-) Versicherungswirtschaft ist zudem aufgrund des für sie geltenden Spartenentrennungsprinzips gezwungen, bestimmte Sparten in verschiedenen Unternehmen zu betreiben, und daher von den mit der derzeitigen datenschutzrechtlichen Situation verbundenen Nachteilen in besonderem Maße betroffen. Sinn der Spartenentrennung ist lediglich eine Trennung der Haftungsmassen im Interesse der Versicherungsnehmer, was einer datenschutzrechtlichen Regelung der Datenverarbeitung im Konzern nicht im Wege steht.

Eine Regelung zur Datenübermittlung in Konzernen ist daher dringend erforderlich.

2.5 Territorialer Anwendungsbereich des europäischen Datenschutzrechts

Unterschiedliche Aussagen in den verschiedenen Sprachfassungen (Art. 3 Abs. 3) und die Erwähnung des Auftragsverarbeiters in Art. 3 Abs. 1 führen zu Unklarheiten, inwieweit die vorgeschlagene Verordnung auf die oben bei 1.5 beschriebenen Sachverhalte anwendbar ist. Nach derzeitiger Rechtslage in Deutschland muss der Auftraggeber im Drittstaat nach Auffassung der deutschen Datenschutzaufsichtsbehörden lediglich die Grenzen des ordre public beachten, darüber hinaus kommt das deutsche Datenschutzrecht nicht zur Anwendung. Für eine künftig weitergehende Erstreckung des EU-

Datenschutzrechts fehlt es aus unserer Sicht an angemessenen Anknüpfungspunkten. Im Hinblick auf IT-Hosting, Cloud Computing u.ä. wären für europäische Dienstleister (einschließlich internationaler Konzerne mit Hauptsitz in der EU) zudem Standortvorteile zu befürchten.

2.6 Zuständigkeit der Aufsichtsbehörde

Europaweit tätigen Unternehmen wie Munich Re ermöglicht der one-stop-shop-Ansatz, künftig Meldungen, Genehmigungs- und Dokumentationsanforderungen für sich und ihre Niederlassungen nur noch einmal zentral bei der zuständigen Datenschutzbehörde zu erfüllen, und sorgt damit für spürbare Erleichterungen.

Nicht erfasst von diesen Erleichterungen wird allerdings, wenn das Unternehmen in einem anderen Mitgliedstaat durch ein Tochterunternehmen anstelle einer Niederlassung vertreten ist. Dieses Tochterunternehmen muss dann die für in der Unternehmensgruppe einheitlichen Verfahren erforderlichen Meldepflichten, Genehmigungs-/ Dokumentationsanforderungen etc. jeweils zusätzlich noch einmal bei seiner lokal zuständigen Aufsichtsbehörde erfüllen. Selbst Binding Corporate Rules nach Art. 43 des Verordnungsvorschlags müssten wohl nicht nur von der Konzernmutter zur Genehmigung bei der zuständigen Aufsichtsbehörde eingereicht werden, sondern auch von den Tochtergesellschaften in anderen EU-Mitgliedstaaten bei den jeweils für sie zuständigen Behörden.

Art. 51 Abs. 2 des Vorschlags sollte daher auch auf Tochterunternehmen einer Unternehmensgruppe (Art. 4 Abs. 16 des Vorschlags) erstreckt werden.

Dr. Wolfgang Mörlin
Tel.: +49 (89) 3891-9853
Fax: +49 (89) 3891-79853
wmoerlin@munichre.com

Münchener Rückversicherungs-Gesellschaft
Aktiengesellschaft in München
Königinstraße 107, 80802 München