

Antwort der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Jan Korte, Nicole Gohlke, Ulla Jelpke,
weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/11122 –**

Umgang von Versicherungskonzernen mit sensiblen Kundendaten

Vorbemerkung der Fragesteller

In seinem 23. Tätigkeitsbericht zum Datenschutz für die Jahre 2009 und 2010 stellte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) einmal mehr fest, dass „die Verbesserung des Datenschutzes bei Versicherungsunternehmen [...] nur langsam voran“ kommt. Bereits mehrfach musste der BfDI massive datenschutzrechtliche Bedenken unter anderem gegen das Hinweis- und Informationssystem (HIS) der Versicherungswirtschaft, das der Risikoprüfung und Aufdeckung bzw. Verhinderung von Versicherungsbetrug dient, thematisieren (vgl. hierzu 22. Tätigkeitsbericht Nummer 4.4.7 und 23. Tätigkeitsbericht Nummer 10.7). Der HIS-Neukonzeption, deren Beratungen zwischen dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) und den Datenschutzaufsichtsbehörden bei Redaktionsschluss des 23. Tätigkeitsberichtes noch nicht abgeschlossen waren, hätten die Datenschutzaufsichtsbehörden nach Darstellung des BfDI nicht zustimmen können und Nachbesserungen gefordert sowie wesentliche datenschutzrechtliche Anforderungen formuliert (vgl. 23. Tätigkeitsbericht, S. 117).

Medienberichten zufolge erhielt die Redaktion von „SPIEGEL ONLINE“ Mitte August 2012 ein anonymes Schreiben, das unter anderem polizeiliche und staatsanwaltschaftliche Ermittlungsakten, Papiere der Dresdner Bank über verschiedene Konten und deren Verfügungsberechtigte oder auch Asylbescheinigungen beinhaltete – alle Schriftstücke enthielten sowohl die Klarnamen von Beteiligten als auch jene von unbeteiligten Personen. Wie sich herausstellte, stammten die Unterlagen aus dem Datensystem des Allianz Versicherungskonzerns, der diese an einen externen Ermittler weiterreichte, um Fälle von Versicherungsbetrug aufzudecken. Laut dem Konzern wurde die Zusammenarbeit mit der Detektei bereits 2011 aufgekündigt. Ob diese die ihr zugesandten sensiblen Datensätze daraufhin ordnungsgemäß vernichtete, wurde offenbar nicht kontrolliert.

Dass Versicherungen Unmengen von Daten sensibelster Art besitzen und speichern, ist nichts Neues. Jedoch stellt sich nun die Frage, ob sie in der Lage sind, den sachgemäßen Umgang mit den Daten zu gewährleisten. Der aktuelle Vorfall ist dabei nur einer von vielen. So waren bereits in den Jahren 2009 und 2010 rund 39 000 Datensätze von Kundinnen und Kunden des Finanzvertriebes AWD an den Norddeutschen Rundfunk gelangt.

Dass Versicherungen in begründeten Betrugsfällen Privatermittler beauftragen, sei völlig in Ordnung, sagte Thomas Kranig, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht. Laut Dr. Thilo Weichert, Datenschutzbeauftragter des Landes Schleswig-Holstein, dürfen Daten jedoch nur im Einzelfall weitergeben werden, etwa im Verdachtsfall von Versicherungsbetrug. Laut der Allianz kommt dies bei 1 000 von rund 3,3 Millionen Schadensfällen im Jahr vor.

Im Falle einer Datenweitergabe an Externe gelangen die Privatermittler jedoch in den Besitz von hochsensiblen und umfangreichen Informationen. Die Detekteien erhalten beispielsweise alle den Fall betreffenden Ermittlungsakten von der Polizei und vom Staatsanwalt. Auch die Zeugenaussagen, die dabei getätigt wurden, werden den Ermittlern zur Verfügung gestellt. So haben sie nicht nur Einsicht in die Privatsphäre des Versicherungsnehmers, sondern auch in die von völlig Unbeteiligten. Was schließlich passiert, wenn die externen Ermittler nicht ordnungsgemäß mit den Daten umgehen und ihre Auftraggeber offenbar versäumen, dies zu gewährleisten, zeigt der Fall des Datenlecks bei der Allianz. Nun stellt sich die Frage, inwieweit der Gesetzgeber hier aktiv werden kann und muss.

1. Wurde die im 23. Tätigkeitsbericht des BfDI erwähnte Neufassung der Einwilligung- und Schweigepflichtentbindungserklärung beschlossen und umgesetzt?

Wenn ja, wann, und mit welchem Inhalt geschah dies?

Wenn nein, warum nicht, und wann rechnet die Bundesregierung mit einem Zustandekommen?

2. Wurden nach Kenntnis der Bundesregierung die Verhandlungen zwischen dem GDV und den Datenschutzaufsichtsbehörden über das neue HIS mittlerweile abgeschlossen?

Wenn ja, wann war das?

Wenn nein, warum nicht?

3. Wurden die datenschutzrechtlichen Bedingungen der Datenschutzaufsichtsbehörden im neuen HIS berücksichtigt?

a) Wenn ja, in welcher Form?

- Wurde das neue HIS als Auskunft auf der Grundlage von § 29 des Bundesdatenschutzgesetzes (BDSG) ausgestaltet?
- Wurde sichergestellt, dass Einmeldungen in die Auskunft nur bei Vorliegen einer Rechtsvorschrift und nicht auf der Grundlage von Einwilligungserklärungen erfolgen dürfen?
- Wurde im HIS geregelt, dass die gespeicherten Daten nur bei Vorliegen eines berechtigten Interesses abgefragt werden dürfen?
- Wurde im HIS geregelt, wie größtmögliche Transparenz für die Versicherungsnehmer und sonstige Betroffene hergestellt wird, und wenn ja, in welcher Form?
- Sieht die Neufassung des HIS vor, dass die Einmeldekriterien ständig zu evaluieren sind?
- Wurde eine Ombudsstelle eingerichtet, die bei versicherungsrechtlichen Zweifelsfragen eingeschaltet werden kann und diese Fragen klärt?
- Sind die Versicherer durch die HIS-Neufassung dazu verpflichtet, strenge Compliance-Regelungen einzuhalten, und wenn ja, welche sind dies?

b) Wenn nein, warum nicht?

Es gibt keine versicherungsaufsichtsrechtliche Verpflichtung zur Verwendung einer bestimmten Einwilligung- und Schweigepflichtentbindungserklärung. Der Düsseldorfer Kreis (die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich) hat sich dafür eingesetzt, die Einwilligung- und

Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft transparenter zu gestalten. Gemeinsam mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. (GDV) haben die Datenschutzaufsichtsbehörden eine Mustererklärung für eine Einwilligungs- und Schweigepflichtentbindungserklärung für die Erhebung und Verwendung von Gesundheitsdaten und sonstiger nach § 203 des Strafgesetzbuches (StGB) geschützter Daten erarbeitet. Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen. Der Düsseldorfer Kreis hat die Mustererklärung mit Wirkung vom 17. Januar 2012 beschlossen. Der Beschluss kann unter anderem auf der Homepage des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI – www.bfdi.bund.de) abgerufen werden.

Der BfDI hat der Bundesregierung ergänzend folgendes mitgeteilt: „Das von der Versicherungswirtschaft für die verschiedenen Versicherungssparten eingeführte Hinweis- und Informationssystem (HIS) wird seit dem 1. April 2011 als Auskunftsei von der Firma Informa Insurance Risk and Fraud Prevention GmbH in Baden-Baden betrieben. Antrags- und Leistungsbereich sowie die einzelnen Versicherungssparten sind streng voneinander getrennt.

In das HIS werden Auffälligkeiten aus Versicherungsfällen gemeldet, z. B. atypische Schadenhäufigkeiten, besondere Schadenfolgen, erschwerte Risiken. Die Versicherungen können Informationen zur Risikoprüfung im Antragsbereich und zur Schadensfallprüfung im Leistungsbereich abrufen. Sämtliche Abfragen werden protokolliert und stichprobenartig überprüft.

Das System wurde in enger Abstimmung zwischen dem GDV und der AG Versicherungswirtschaft des Düsseldorfer Kreises konzipiert. Rechtsgrundlagen sind für die Einmeldung personenbezogener Daten in das System § 28 Absatz 1 Nummer 2 des Bundesdatenschutzgesetzes (BDSG) und für die geschäftsmäßige Erhebung und Speicherung zum Zweck der Übermittlung § 29 BDSG. Bei HIS ist eine Einwilligung der Betroffenen zur Einmeldung von Daten nicht erforderlich, weil für die Datenübermittlung an die Auskunftsei mit § 28 Absatz 1 Nummer 2 BDSG ein gesetzlicher Erlaubnistatbestand vorhanden ist.

Die AG Versicherungswirtschaft ist nach eingehender Prüfung zu dem Schluss gekommen, dass die Nutzung von HIS zur Wahrung berechtigter Interessen der Versicherungsunternehmen erforderlich ist und unter Berücksichtigung der Ausgestaltung des Systems kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung überwiegt. Die für die Auskunftsei in Baden-Baden zuständige baden-württembergische Datenschutzaufsichtsbehörde hat sich vor der Inbetriebnahme des Systems davon überzeugt, dass HIS den datenschutzrechtlichen Anforderungen Rechnung trägt. In Zweifelsfällen können sich Betroffene an den Landesbeauftragten für den Datenschutz Baden-Württemberg als zuständige Datenschutzaufsichtsbehörde wenden.

In der Versicherungswirtschaft ist eine unabhängige Schlichtungsstelle in Form eines Versicherungsombudsmanns eingerichtet. Der Ombudsmann ist Prof. Dr. Günter Hirsch. Flankiert wird die Einwilligungs- und Schweigepflichtentbindungserklärung durch Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft (Code of Conduct). Während die Erklärung nur für die einwilligungsbedürftigen Datenerhebungs- und -verwendungsprozesse eingeholt werden soll, konkretisiert der Code of Conduct andere Datenverarbeitungen.

Der Düsseldorfer Kreis hat sich nach längeren Verhandlungen mit dem GDV im September dieses Jahres auf die Verhaltensregeln geeinigt. Der GDV hat den Code of Conduct am 18. Oktober 2012 dem zuständigen Berliner Beauftragten für Datenschutz und Informationsfreiheit gemäß § 38a BDSG zur Überprüfung unterbreitet.“

Der Bundesregierung ist nicht bekannt, ob die Neufassung des HIS vorsieht, dass die Einmeldekriterien ständig zu evaluieren sind.

Der GDV unterliegt nicht der Aufsicht der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Die das HIS betreibende Stelle ist kein von der BaFin beaufsichtigtes Unternehmen.

4. Welche Daten – neben den zur Aufnahme notwendigen – ihrer Versicherungsnehmerinnen und -nehmer dürfen Versicherungskonzerne auf welcher gesetzlichen Grundlage wie speichern?

Es gibt hierzu keine spezielle versicherungsaufsichtsrechtliche Regelung. Für die Speicherung personenbezogener Daten gilt das BDSG.

5. Wer hat auf die bei Versicherungskonzernen gespeicherten sensiblen Kundendaten Zugriff?

Sobald die Staatsanwaltschaft durch eine Anzeige oder auf anderem Wege von dem Verdacht einer Straftat Kenntnis erhält, hat sie zu ihrer Entschließung darüber, ob die öffentliche Klage zu erheben ist, den Sachverhalt zu erforschen. Dabei kann sie die Ermittlungen auch durch die Behörden und Beamten des Polizeidienstes vornehmen lassen (§ 160 Absatz 1 der Strafprozessordnung – StPO). Soweit für die Erforschung des Sachverhalts erforderlich, können die Staatsanwaltschaft und die Polizei in einem zum Beispiel gegen einen Versicherungsnehmer anhängigen Strafverfahren von einem Versicherungskonzern nach Maßgabe der einschlägigen gesetzlichen Vorschriften Auskunft zu den über einen Versicherungsnehmer gespeicherten Daten verlangen (§ 161 Absatz 1, § 163 Absatz 1 StPO). Bei Verweigerung der Auskunft kann nach Maßgabe der gesetzlichen Bestimmungen eine förmliche Vernehmung als Zeuge erzwungen (§§ 161a, 51 StPO) und im Übrigen die Herausgabe der Daten verlangt (§ 95 StPO) oder die Durchsuchung (§§ 103 ff. StPO) und Beschlagnahme (§§ 94 ff. StPO) angeordnet werden.

Die BaFin hat Auskunftsrechte gemäß § 83 des Versicherungsaufsichtsgesetzes (VAG) und unterliegt der Schweigepflicht gemäß § 84 VAG.

6. Auf welcher gesetzlichen Grundlage und mit welcher Begründung haben Versicherungskonzerne Zugriff auf die gesamten zur Versicherungsnehmerin bzw. zum Versicherungsnehmer gehörenden polizeilichen und staatsanwaltlichen Akten?

Ist ein Versicherungskonzern durch die Straftat eines seiner Versicherungsnehmer in eigenen Rechten verletzt, kann ein Rechtsanwalt die Akten des gegen diesen Versicherungsnehmer anhängigen Strafverfahrens, die dem Gericht vorliegen oder diesem im Falle der Erhebung der öffentlichen Klage vorzulegen wären, einsehen, soweit er hierfür ein berechtigtes Interesse, wie etwa die Durchsetzung zivilrechtlicher Forderungen gegen den Versicherungsnehmer, darlegt (§ 406e Absatz 1 Satz 1 StPO). Die Einsicht in die Akten ist zu versagen, soweit überwiegende schutzwürdige Interessen des Beschuldigten oder anderer Personen entgegenstehen (§ 406e Absatz 2 Satz 1 StPO). Auf Antrag können dem Rechtsanwalt, soweit nicht wichtige Gründe entgegenstehen, die Akten mit Ausnahme der Beweisstücke in seine Geschäftsräume oder seine Wohnung mitgegeben werden (§ 406e Absatz 3 Satz 1 StPO). Dem Versicherungskonzern, der ein berechtigtes Interesse darlegt, können auch ohne Einschaltung eines Rechtsanwalts Auskünfte oder Abschriften aus den Akten erteilt werden (§ 406e Absatz 5 erster Halbsatz StPO). Die erlangten personenbezogenen Daten dürften

nur zu dem Zweck verwendet werden, für den die Auskunft oder Akteneinsicht gewährt wurde. Eine Verwendung für andere Zwecke ist zulässig, wenn dafür Auskunft oder Akteneinsicht gewährt werden dürfte und die Stelle, die Auskunft oder Akteneinsicht gewährt hat, zustimmt. Wird eine Auskunft ohne Einschaltung eines Rechtsanwalts erteilt, so ist auf die Zweckbindung hinzuweisen (§ 406e Absatz 6 in Verbindung mit § 477 Absatz 5 StPO).

Ist nicht der Versicherungskonzern, sondern einer seiner Versicherungsnehmer Verletzter einer von einem Dritten begangenen Straftat, kann ein von dem Versicherungskonzern beauftragter Rechtsanwalt Auskünfte aus den Akten, die dem Gericht vorliegen oder diesem im Falle der Erhebung der gegen den Dritten gerichteten öffentlichen Klage vorzulegen wären, erhalten, soweit er hierfür ein berechtigtes Interesse, wie etwa die Durchsetzung zivilrechtlicher Regressforderungen gegen den Dritten, darlegt (§ 475 Absatz 1 Satz 1 StPO). Auskünfte sind zu versagen, wenn der hiervon Betroffene ein schutzwürdiges Interesse an der Versagung hat (§ 475 Absatz 1 Satz 2 StPO). Soweit der Rechtsanwalt ein berechtigtes Interesse darlegt, kann ihm Akteneinsicht gewährt werden, wenn die Erteilung von Auskünften einen unverhältnismäßigen Aufwand erfordern oder nach Darlegung dessen, der Akteneinsicht begehrt, zur Wahrnehmung des berechtigten Interesses nicht ausreichen würde (§ 475 Absatz 2 StPO). Auf Antrag können dem Rechtsanwalt, soweit Akteneinsicht gewährt wird und nicht wichtige Gründe entgegenstehen, die Akten mit Ausnahme der Beweisstücke in seine Geschäftsräume oder seine Wohnung mitgegeben werden (§ 475 Absatz 3 Satz 2 StPO). Dem Versicherungskonzern, der ein berechtigtes Interesse darlegt, können auch ohne Einschaltung eines Rechtsanwalts Auskünfte aus den Akten erteilt werden (§ 475 Absatz 4 StPO). Die erlangten personenbezogenen Daten dürften nur zu dem Zweck verwendet werden, für den die Auskunft oder Akteneinsicht gewährt wurde. Eine Verwendung für andere Zwecke ist zulässig, wenn dafür Auskunft oder Akteneinsicht gewährt werden dürfte und die Stelle, die Auskunft oder Akteneinsicht gewährt hat, zustimmt. Wird eine Auskunft ohne Einschaltung eines Rechtsanwalts erteilt, so ist auf die Zweckbindung hinzuweisen (§ 477 Absatz 5 StPO).

7. Auf welche Daten welcher Behörden und Institutionen haben Versicherungen mit welcher Begründung im Falle des Auftretts eines Schadens Zugriff?

Im Falle eines Schadens bei einem Versicherungsunternehmen als Folge einer Straftat kommen die in der Antwort zu Frage 6 dargestellten Auskunfts- und Akteneinsichtsmöglichkeiten in Betracht.

8. Ist der Bundesregierung bekannt, in wie vielen und welchen Fällen Versicherungskonzerne jährlich Detekteien beauftragen und dabei mit sensiblen Kundendaten ausstatten?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor. Es besteht keine entsprechende Meldepflicht gegenüber der BaFin.

9. Welche Schlussfolgerungen zieht die Bundesregierung aus der Tatsache, dass der GDV ein externes Unternehmen mit der Führung des neuen HIS beauftragt hat?

Auf die Antwort zu den Fragen 1 bis 3 wird verwiesen.

10. Auf welcher gesetzlichen Grundlage ist es den Versicherungen unter welchen Voraussetzungen erlaubt, Daten ihrer Kundinnen und Kunden an externe Dienstleister weiterzugeben?

Bei der Auslagerung von Dienstleistungen sind die Bestimmungen des Gesetzes über die Beaufsichtigung der Versicherungsunternehmen (VAG), insbesondere § 64a VAG, zu beachten. Versicherungsunternehmen müssen über eine ordnungsgemäße Geschäftsorganisation verfügen, welche die Einhaltung der von ihnen zu beachtenden Gesetze und Verordnungen sowie der aufsichtsbehördlichen Anforderungen auch bei der Auslagerung von Dienstleistungen gewährleistet. Darunter fällt auch die Beachtung des BDSG.

Zu beachten ist jedoch, dass die BaFin nur die gemäß § 64a VAG geforderten allgemeinen organisatorischen Vorgaben überprüfen kann. Die Überprüfung, ob die Vorgaben des Bundesdatenschutzgesetzes im Einzelfall eingehalten sind, obliegt den zuständigen Datenschutzaufsichtsbehörden.

11. Welche Voraussetzungen müssen für die Annahme eines konkreten Verdachtes eines Versicherungsbetruges und somit für die Erlaubnis einer Datenweitergabe an Dritte durch Versicherungskonzerne vorliegen?

Der Verdacht eines Betruges zum Nachteil eines Versicherungskonzerns oder der Verdacht eines Versicherungsmissbrauchs (§§ 263, 265 des Strafgesetzbuches) setzt jeweils zureichende tatsächliche Anhaltspunkte für das Vorliegen einer solchen Straftat (§ 152 Absatz 2 StPO) voraus. Ob solche Anhaltspunkte bestehen, hängt von den konkreten Umständen des Einzelfalls ab und entzieht sich einer generalisierenden Betrachtung.

Die (Un-)Zulässigkeit der Weitergabe von Daten aus einem Strafverfahren an Dritte hängt insbesondere von dem Zweck ab, für den Akteneinsicht oder Auskunft gewährt worden ist. Insoweit wird auf die Antwort zu Frage 6 zur Zweckbindung verwiesen.

12. Wie beurteilt die Bundesregierung die Tatsache, dass es Versicherungen vor dem Hintergrund der Weitergabe höchstsensibler Daten ihrer Kundinnen und Kunden gestattet ist, externe Ermittler zu beauftragen?

Den Versicherungsunternehmen ist es im Rahmen der versicherungsaufsichtsrechtlichen Vorschriften gestattet, zur Wahrung ihrer berechtigten Interessen externe Ermittler einzuschalten, wenn und soweit die insofern anwendbaren datenschutzrechtlichen Bestimmungen eingehalten sind.

13. Hält die Bundesregierung die Praxis der Versicherungskonzerne – vor dem Hintergrund des Allianz-Vorfalles – für gerechtfertigt?
Wenn ja, mit welcher Begründung?
Wenn nein, warum nicht?

Auf die Antwort zu Frage 12 wird verwiesen.

14. Gibt es bei der Weitergabe von Daten durch Versicherungskonzerne Regelungen hinsichtlich Daten, die unter keinen Umständen an Dritte weitergegeben werden dürfen?
Wenn ja, welche Regelungen sind das, und welche Art von Daten ist davon betroffen?

Es gibt keine derartigen Regelungen.

15. Ist der Bundesregierung bekannt, ob die Versicherungsnehmerinnen und -nehmer im Falle einer Datenweitergabe an Dritte informiert werden müssen, informiert werden oder eine Einwilligung erteilen müssen?

Auf die Antwort zu Frage 10 wird verwiesen.

16. Ist der Bundesregierung bekannt, ob und wie Versicherungskonzerne die Arbeit der von ihnen beauftragen externen Dienstleister kontrollieren bzw. kontrollieren können?

Die Versicherungsunternehmen sind verpflichtet, im Rahmen der Auslagerung von Tätigkeiten auch die Datenschutzbestimmungen zu beachten und haben sich auch Prüfungsrechte vertraglich vorzubehalten. Die ausgelagerte Dienstleistung ist im Hinblick auf das Erfordernis, eine ordnungsgemäße Geschäftsorganisation und ein angemessenes Risikomanagement vorzuhalten (§ 64a Absatz 1 VAG), vom jeweiligen Versicherungsunternehmen auch ausreichend zu kontrollieren. Die Kontrollen haben dabei auch die ordnungs- und auftragsgemäße Leistungserbringung einzubeziehen. Darüber hinaus hat die Interne Revision des Versicherungsunternehmens auch die ausgelagerten Geschäftsbereiche mit in ihre Prüftätigkeit einzubeziehen.

17. Welche Regelungen gelten für die durch Versicherungskonzerne beauftragten Dritten hinsichtlich Datenverarbeitung, Datenaufbewahrung und Datenvernichtung?

Durch die Auslagerung von Tätigkeiten auf Dritte dürfen die im Versicherungsaufsichtsgesetz gestellten Anforderungen nicht abgesenkt werden, so dass diese auch mittelbar für Dritte gelten. Es sind ferner die datenschutzrechtlichen Bestimmungen einzuhalten.

