Deutscher Bundestag **Drucksache 18/321**

18. Wahlperiode 21.01.2014

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Axel Troost, Susanna Karawanskij, Klaus Ernst, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/225 –

Datenschutz bei der Zusammenarbeit deutscher Finanzdienstleister mit IT-Unternehmen insbesondere aus den USA vor dem Hintergrund des NSA-Skandals

Vorbemerkung der Fragesteller

Die Allianz SE, das weltgrößte Versicherungsunternehmen, möchte zukünftig ihre Rechenzentren auslagern und an das amerikanische IT-Unternehmen IBM übergeben. Dies wirft unter anderem datenschutzrechtliche sowie verbraucherschutzpolitische Probleme auf, denn im Zuge der NSA-Affäre steht die glaubwürdige Behauptung, der amerikanische Geheimdienst NSA habe mit vielen US-amerikanischen Herstellern von Computersoftware und -hardware und vielen IT-Dienstleistern geheime Abkommen, die der NSA Zugang zu deren Datennetzwerken eröffnen, im Raum. Es kann derzeit nicht ausgeschlossen werden, dass die NSA über amerikanische Unternehmen wie IBM Zugriff auf sensible Daten deutscher Kreditinstituts- und Versicherungskunden erhält. Deutsche Unternehmen müssen aber von Gesetzes wegen den Schutz der Daten ihrer Kunden sicherstellen und unterliegen dabei erheblichen Sorgfaltspflichten. Der Landesbeauftragte für den Datenschutz Schleswig-Holstein, Dr. Thilo Weichert, äußerte daher bereits starke Bedenken: „Angesichts der Erkenntnisse um die Ausspähaktionen durch US-Geheimdienste wäre es unverantwortlich, europäische Kundendaten in den USA verarbeiten zu lassen“ (taz.die tageszeitung vom 26. November 2013).

1. Ist es aus Sicht der Bundesregierung im Sinne der einschlägigen Gesetzeslage (z. B. Bundesdatenschutzgesetz, aber auch finanzsektorspezifische Regulierungen wie z. B. die Mindestanforderungen an das Risikomanagement – MaRisk) ausreichend, wenn ein Finanzdienstleistungsunternehmen seine Kooperation mit einem externen IT-Dienstleister, der im Auftrag des Finanzdienstleistungsunternehmens Daten verarbeitet, erst dann auf den Prüfstand stellt, wenn diesem externen Dienstleister Verletzungen des Datenschutzes nachgewiesen bzw. von diesem eingestanden wurden, oder gebieten die Sorgfaltspflichten, dass das Finanzdienstleistungsunternehmen die Kooperation mit dem externen IT-Dienstleister auch schon bei einem be-

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Finanzen vom 17. Januar 2014 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

gründeten Verdacht auf Datenschutzverletzungen (z. B. im Fall behördlicher Ermittlungen oder Offenlegungen durch Whistleblower) auf den Prüfstand stellen?

Maßgebend sind die Regelungen in § 11 des Bundesdatenschutzgesetzes (BDSG), der bereits jetzt regelt, dass bei Vertragsabschluss hinreichende Regelungen zu Maßnahmen gemäß § 9 BDSG nebst Anlage detailliert dargelegt werden müssen. Weiterhin fordert § 11 Absatz 2 Satz 2 Nummer 3 BDSG, dass der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen ist. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere die nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen festzulegen sind. Nach § 11 Absatz 2 Satz 4 BDSG hat sich der Auftraggeber vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren. Diese Regelung setzt also voraus, dass vor Beginn der Verarbeitung eine Prüfung stattfindet.

2. Ab welchem Umfang von datenschutzrechtlichen Verfehlungen eines beauftragten IT-Dienstleisters ist ein Finanzdienstleistungsunternehmen verpflichtet, die Kooperation mit diesem IT-Dienstleister unverzüglich zu beenden, und wie groß ist der Ermessensspielraum des Finanzdienstleistungsunternehmens bei dieser Entscheidung?

Datenschutzrechtliche Verfehlungen lassen sich nicht einfach quantifizieren. Die Einhaltung des BDSG sowie anderer Vorschriften über den Datenschutz liegt in der Verantwortung der Personen, die das Unternehmen vertreten. Sie werden dabei von der zuständigen Aufsichtsbehörde kontrolliert, § 38 Absatz 1 BDSG.

3. Welche Rolle spielt es für die Beantwortung der Fragen 1 und 2, ob der externe IT-Dienstleister seine Dienstleistung im In- bzw. Ausland erbringt oder seinen Sitz im In- bzw. Ausland hat?

   Welche Rolle spielt der Unterschied zwischen EU-Ausland, Drittstaaten im Allgemeinen und den USA im Besonderen, und welche Rolle spielt in diesem Zusammenhang jeweils der § 11 des Bundesdatenschutzgesetzes (BDSG)?

Unabhängig davon, ob der externe IT-Dienstleister seine Dienstleistung im In- bzw. Ausland erbringt oder seinen Sitz im In-bzw. Ausland hat, bleibt das beauftragende Finanzdienstleistungsunternehmen weiterhin verantwortliche Stelle im Sinne des § 3 Absatz 7 BDSG und damit den Verpflichtungen des § 11 BDSG und der Kontrolle durch die zuständige Aufsichtsbehörde unterworfen.

Ein Datentransfer in einen Drittstaat ist nach den Vorschriften der Artikel 25 und 26 der Europäischen Datenschutzrichtlinie verboten, wenn dieser über kein dem EU-Recht vergleichbares Datenschutzniveau verfügt. Dies trifft auf die USA zu, da es dort keine umfassenden gesetzlichen Regelungen zum Datenschutz gibt, die dem europäischen Standard entsprechen. Allerdings sieht Artikel 25 Absatz 6 der Richtlinie vor, dass die Kommission der Europäischen Gemeinschaft die Angemessenheit des Datenschutzes in einem Drittland feststellen kann, wenn dieses bestimmte Anforderungen erfüllt.

Zu diesem Zweck wurde das so genannte Safe-Harbor-Modell entwickelt. Bei „Safe Harbor“ handelt es sich um eine zwischen der Europäischen Union und den USA im Jahr 2000 getroffene Vereinbarung, die gewährleistet, dass personenbezogene Daten legal in die USA übermittelt werden können. In den USA

tätige Unternehmen, die sich dem „Safe-Harbor“-Modell angeschlossen haben, sind vor der Sperrung des Datenverkehrs sicher, andererseits wissen europäische Unternehmen, die personenbezogene Daten an in den USA tätige Firmen übermitteln, dass sie keine zusätzlichen Garantien verlangen müssen. Die Prüfpflichten der verantwortlichen Stellen auf deutscher Seite vor einer Übermittlung personenbezogener Daten in die USA bleiben jedoch bestehen.

4. Ist es aus Sicht der Bundesregierung generell zulässig, sensible Finanzdaten deutscher Bank- und Versicherungskunden an ausländische IT-Dienstleister weiterzugeben, wenn diese nicht denselben gesetzlichen Datenschutzbestimmungen wie in Deutschland unterliegen, und welche Rolle spielt hierbei, ob es sich um EU-Mitglieds- oder Drittstaaten handelt (bitte begründen)?

Zu den datenschutzrechtlichen Aspekten wird auf die Antwort zu Frage 3 verwiesen.

5. Wenn ja, welche rechtlichen (insbesondere datenschutzrechtlichen) Einschränkungen sind bei einer solchen Auslagerung zu beachten?

Auf die Antwort zu Frage 4 wird verwiesen.

6. Wenn nein, wie gedenkt die Bundesregierung gegen eine solche Auslagerung vorzugehen, und welche Rolle spielt hierbei, ob es sich um EU-Mitglied- oder Drittstaaten handelt?

Auf die Antwort zu Frage 4 wird verwiesen.

7. Teilt die Bundesregierung die Aussage des Landesbeauftragten für den Datenschutz Schleswig-Holstein, Dr. Thilo Weichert, „Angesichts der Erkenntnisse um die Ausspähaktionen durch US-Geheimdienste wäre es unverantwortlich, europäische Kundendaten in den USA verarbeiten zu lassen“ (taz.die tageszeitung vom 26. November 2013)?

   Wenn nein, warum nicht?

Zuständig ist jeweils die Datenschutzaufsichtsbehörde des Landes, in dem das Finanzdienstleistungsunternehmen seinen Sitz hat. Diese ist in ihrer Aufgabenerfüllung völlig unabhängig. Dies umfasst auch die Bewertung der Einhaltung datenschutzrechtlicher Regelungen durch nichtöffentliche Stellen, weshalb die Bundesregierung von einer öffentlichen Stellungnahme absieht.

8. Welche Behörden sind für die Überprüfung der Einhaltung der datenschutzrechtlichen Bestimmungen seitens Finanzdienstleistungsunternehmen zuständig, und welche Kontrollinstrumente stehen diesen Behörden zur Verfügung?

Die Kontrolle der Einhaltung der datenschutzrechtlichen Bestimmungen obliegt den zuständigen Aufsichtsbehörden, § 38 BDSG. Dies sind für den nichtöffentlichen Bereich die Datenschutzaufsichtsbehörden der Länder. Ihnen stehen die Kontroll- und Sanktionsmöglichkeiten des BDSG zur Verfügung.

9. Welche Rolle kommt bei der Überprüfung des Datenschutzes der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), z. B. im Rahmen der Aufsicht über die Einhaltung der MaRisk, zu?

Die BaFin hat grundsätzlich keine direkte Zuständigkeit für die Einhaltung von datenschutzrechtlichen Regelungen. Sie erwartet von den von ihr beaufsichtigten Unternehmen, dass sie die datenschutzrechtlichen Vorgaben erfüllen. Sie berücksichtigt Datenschutzverstöße im Rahmen ihrer aufsichtsrechtlichen Tätigkeit, sofern sie auf eine nicht ordnungsgemäße Geschäftsorganisation hindeuten.

In der Bankenaufsicht gilt, dass gemäß Abschnitt AT 7.2 Tz. 2 der Mindestanforderungen an das Risikomanagement (MaRisk-Rundschreiben 10/2012) die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen müssen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen, insbesondere sind Prozesse für eine angemessene IT-Berechtigungsvergabe einzurichten, die sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt. Die Eignung der IT-Systeme und der zugehörigen Prozesse ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.

Soweit ein Finanzdienstleistungsinstitut Daten bzw. die Verarbeitung seiner Daten auslagert, hat das Institut gemäß Abschnitt AT 9 Tz. 6e MaRisk im Auslagerungsvertrag sicherzustellen, dass das Unternehmen, an welche das Institut auslagert, die datenschutzrechtlichen Bestimmungen beachtet. Die Einhaltung dieser Vorschrift wird von der Aufsicht ebenfalls überwacht.

Für die übrigen Aufsichtsbereiche gelten weitgehend analoge Regelungen, etwa für Versicherer: § 64a des Versicherungsaufsichtsgesetzes und Rundschreiben 3/2009 [VA] zu den Mindestanforderungen an das Risikomanagement; § 33 des Wertpapierhandelsgesetzes in Verbindung mit § 25a des Kreditwesengesetzes und Rundschreiben 5/2010 [WA] zu den Mindestanforderungen an das Risikomanagement für Investmentgesellschaften (InvMaRisk). Nach den letztgenannten Vorschriften müssen Kapitalverwaltungsgesellschaften interne Organisationsrichtlinien erstellen und beachten, welche Regelungen beinhalten, die die Einhaltung gesetzlicher Bestimmungen sowie sonstiger Vorgaben (z. B. Datenschutz) gewährleisten (Nummer 5 Ziffer 3k InvMaRisk). Zudem legt Nummer 9 Ziffer 6e InvMaRisk fest, dass bei Auslagerungen im Auslagerungsvertrag insbesondere Regelungen, die sicherstellen, dass datenschutzrechtliche Bestimmungen beachtet werden, vereinbart werden.

Die Aufsicht erwartet, dass sich Institute auch mit sich abzeichnenden Risiken auseinandersetzen und nicht erst, wenn Unternehmen Mängel im Datenschutz nachgewiesen werden. Die BaFin kann nach den oben beispielhaft genannten gesetzlichen Regelungen Datenschutzverstößen der Institute nachgehen, wenn diese Anhaltspunkte für Defizite im Hinblick auf eine ordnungsgemäße Geschäftsorganisation bieten.

10. Spielen bei der Überwachung des Datenschutzes durch Aufsichtsbehörden ausschließlich kundenbezogene Aspekte (Persönlichkeitsrechte etc.) eine Rolle, oder kann aus Sicht der Bundesregierung die Nichteinhaltung datenschutzrechtlicher Verpflichtungen durch Finanzdienstleistungsunternehmen auch eine Gefährdung eines oder mehrerer Finanzdienstleistungsunternehmen oder sogar systemische Risiken für die Stabilität des Finanzsektors insgesamt zur Folge haben?

Auf die Antwort zu Frage 8 wird verwiesen. Die Datenschutzaufsichtsbehörden der Länder sind in ihrer Aufgabenerfüllung völlig unabhängig.

Derzeit liegen der Bundesregierung keine Erkenntnisse vor, dass die Nichteinhaltung datenschutzrechtlicher Verpflichtungen durch Finanzdienstleistungsunternehmen auch eine Gefährdung eines oder mehrerer Finanzdienstleistungsunternehmen oder sogar systemische Risiken für die Stabilität des Finanzsektors insgesamt zur Folge haben kann.

11. Wie häufig wird die Einhaltung der datenschutzrechtlichen Bestimmungen von der BaFin oder anderen Behörden durchschnittlich geprüft?

    Bei welchen Finanzdienstleistungsunternehmen wird die Einhaltung der datenschutzrechtlichen Bestimmungen routinemäßig geprüft?

    Bei welchen Finanzdienstleistungsunternehmen bedarf es eines konkreten Anlasses bzw. Anfangsverdachts, damit eine entsprechende Prüfung stattfindet?

Die Überwachung datenschutzrechtlicher Bestimmungen gehört nicht zu den Aufgaben der BaFin und wird mit Ausnahme des in der Antwort zu Frage 9 dargelegten geschäftsorganisatorischen Aspektes nicht geprüft.

Organisatorische Defizite mit Blick auf den Datenschutz wurden der BaFin auch nicht von Wirtschaftsprüfern im Rahmen der jährlichen Berichterstattung über die Einhaltung der regulatorischen Vorgaben (u. a. der diversen MaRisk) mitgeteilt. Vor diesem Hintergrund hat die BaFin bisher keine Veranlassung gehabt, das Thema Datenschutz im Rahmen von Aufsichtsgesprächen oder auf andere Art und Weise besonders zu problematisieren.

12. Wie viele Prüfungen auf Einhaltung datenschutzrechtlicher Bestimmungen hat die BaFin in den vergangenen drei Jahren durchgeführt (bitte nach Kreditinstituten, Versicherungen und Wertpapierdienstleistungsunternehmen aufschlüsseln)?

    Wie viele davon waren routinemäßig, wie viele davon waren anlassbezogen?

Die BaFin hat speziell mit Blick auf die Einhaltung datenschutzrechtlicher Bestimmungen keine Prüfungen bei den von ihr überwachten Instituten durchgeführt.

13. Wie waren die Prüfungsergebnisse (bitte nach Art und Schwere der Beanstandungen aufschlüsseln)?

Auf die Antwort zu Frage 12 wird verwiesen.

14. Wie bewertet die Bundesregierung vor dem Hintergrund der Enthüllungen im NSA-Überwachungsskandal, dass Booz Allen Hamilton, die ehemalige Firma des Whistleblowers Edward Snowden, einen Auftrag des Bundesministeriums der Finanzen zur Organisationsentwicklung der BaFin erhalten hatte (Antwort auf die Schriftliche Frage 11 auf Bundestagsdrucksache 18/115), und sieht sie diesbezüglich sicherheits- und datenschutzrechtliche Probleme (bitte begründen)?

Die BaFin vergibt Aufträge an externe Dienstleister wie Booz Allen Hamilton entsprechend dem geltenden Vergaberecht. Im Rahmen des Vergabeverfahrens wird die Eignung des Dienstleisters mit Blick auf den zu erfüllenden Auftrag überprüft. Zum Zeitpunkt der Auftragsvergabe im Jahr 2003 gab es keine Bedenken gegen die Eignung von Booz Allen Hamilton. Der Auftrag an Booz

Allen Hamilton zielte darauf ab, die Entwicklung von Vorschlägen für die Optimierung der Aufbau- und Ablauforganisation der BaFin zu unterstützen, nicht jedoch Detailfragen der Aufsichtsarbeit einer Überprüfung zu unterziehen.

Die Untersuchung endete mit Empfehlungen zur Aufbau- und Ablauforganisation auf einem hohen Abstraktionsniveau. Für die Konkretisierung der Empfehlungen wurde die Hilfe von Booz Allen Hamilton nicht weiter in Anspruch genommen.

Aus Sicht der BaFin wurden durch die Zusammenarbeit mit Booz Allen Hamilton weder sicherheits- noch datenschutzrechtliche Probleme aufgeworfen.

15. Welche Kreditinstitute, Versicherungen und Wertpapierhandelsunternehmen bedienen sich nach Kenntnis der Bundesregierung zur Verarbeitung ihrer Kundendaten externer IT-Dienstleister?

    An welches Unternehmen erfolgte wann die Auslagerung?

Üblicherweise erfolgt die Verarbeitung von Daten bei externen IT-Dienstleistern auf Grund von Dienstleistungsverträgen, die weder einer Genehmigung bedürfen noch der Aufsichtsbehörde routinemäßig vorgelegt werden müssen. Die Bundesregierung kann die Frage mit den ihr vorliegenden Unterlagen daher nicht beantworten.

16. Wie viele und welche Finanzdienstleistungsunternehmen haben nach Kenntnis der Bundesregierung dabei die Verarbeitung ihrer Kundendaten zu IT-Dienstleistern ins Ausland verlagert?

Auf die Antwort zu Frage 15 wird verwiesen.

17. Sind der Bundesregierung außer der Allianz SE noch weitere Finanzdienstleistungsunternehmen bekannt, die eine Auslagerung ihrer Datenverarbeitung an externe IT-Dienstleister erwägen, und wenn ja, um welche Unternehmen handelt es sich dabei?

Konkrete Angaben zu Finanzdienstleistungsunternehmen, die eine Auslagerung ihrer Datenverarbeitung an externe IT-Dienstleister erwägen, unterliegen als vertrauliche, im Rahmen der aufsichtsrechtlichen Tätigkeit der BaFin zugängliche Informationen der Verschwiegenheitspflicht nach § 84 des Versicherungsaufsichtsgesetzes bzw. § 9 des Kreditwesengesetzes. Das öffentliche Bekanntwerden der erfragten Informationen hat grundsätzlich das Potenzial, die Wettbewerbssituation einzelner Unternehmen zu beeinträchtigen. Nach sorgfältiger Abwägung mit den Informationsrechten des Deutschen Bundestages und seiner Abgeordneten kann in der Sache daher keine Auskunft in der für Kleine Anfragen nach § 104 i. V. m. § 75 Absatz 3, § 76 Absatz 1 der Geschäftsordnung des Deutschen Bundestages (GO BT) vorgesehenen, zur Veröffentlichung in einer Bundestagsdrucksache bestimmten Weise erfolgen. Die Antwort wird deshalb mit Blick auf die einzelne Unternehmen betreffenden Daten eingestuft in der Geheimschutzstelle des Deutschen Bundestages zur Verfügung gestellt.*

* Das Bundesministerium der Finanzen hat die Antwort als „VS – Vertraulich“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

18. Wie beurteilt die Bundesregierung die Möglichkeit sowie die Wahrscheinlichkeit, dass die NSA durch Kooperation mit von deutschen Finanzdienstleistungsunternehmen beauftragten US-amerikanischen IT-Dienstleistern Zugriff auf Daten deutscher Finanzdienstleistungsunternehmen erhalten kann und davon auch Gebrauch macht?

    Haben deutsche Geheimdienste von der NSA Daten deutscher Finanzdienstleistungsunternehmen erhalten?

Ein Zugriff der NSA in Kooperation mit entsprechenden IT-Dienstleistern auf Daten deutscher Finanzdienstleistungsunternehmen ist theoretisch nicht auszuschließen. Allerdings dürfte ein solcher Zugriff regelmäßig rechtswidrig sein. Eine Beurteilung der jeweils betroffenen Rechtsvorschriften ist der Bundesregierung jedoch nur aufgrund konkreter Einzelfälle möglich.

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Beantwortung des zweiten Teils der Frage 18 nicht in offener Form erfolgen kann. Die erbetene Auskunft betrifft im Zusammenhang mit der Aufgabenerfüllung des Bundesnachrichtendienstes stehende Informationen. Einzelheiten zu Kooperationen und zum Informationsaustausch des Bundesnachrichtendienstes mit anderen Nachrichtendiensten unterliegen der vertraulichen Behandlung. Ein Verstoß gegen die in diesem Zusammenhang vorausgesetzte Vertraulichkeit ließe negative Folgewirkungen für die Quantität und Qualität des Informationsaustausches befürchten: ein Rückgang von Informationen wäre wahrscheinlich. In der Konsequenz könnte dies zu einer Verschlechterung der Fähigkeit des Bundesnachrichtendienstes zur Abbildung der Sicherheitslage führen. Darüber hinaus können Angaben zu Art und Umfang des Erkenntnisaustauschs mit ausländischen Nachrichtendiensten auch Rückschlüsse auf Aufklärungsaktivitäten und -schwerpunkte des Bundesnachrichtendienstes zulassen. Eine Kenntnisnahme durch Unbefugte würde daher für die Auftragserfüllung des Bundesnachrichtendienstes insofern erhebliche Nachteile zur Folge haben. Sie könnte die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen. Um dem verfassungsrechtlich verbürgten Frage- und Informationsrecht des Parlaments unter Wahrung der berechtigten Geheimhaltungsinteressen gleichwohl Rechnung zu tragen, sind die entsprechenden Informationen als Verschlusssache gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem VS-Grad „GEHEIM“ eingestuft und werden in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.*

19. Was versteht die Bundesregierung unter dem Terminus „operative Services“, die der IT-Dienstleister aus einem anderen Staat anbietet, insbesondere aus datenschutz- sowie verbraucherschutzpolitischer Perspektive?

Es handelt sich nach Kenntnis der Bundesregierung nicht um einen Begriff, dem sich im Geschäftsverkehr ein konkreter Inhalt zuordnen lässt.

* Das Bundesministerium der Finanzen hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

20. Inwieweit verfügt die Bundesregierung über Kenntnisse, ob und inwieweit deutsche Kundendaten von Kreditinstituten, Versicherungen und Wertpapierhandelsunternehmen in einer so genannten Cloud verarbeitet wurden oder werden, die ihrerseits auch mit Rechenzentren in Staaten verbunden ist, die keinen aus deutscher Sicht hinreichenden Datenschutz sicherstellen?

Unter einer Cloud versteht man einen Verbund externer Speicher- und oder Serversysteme, mit dem entsprechende IT-Dienstleistungen erbracht werden.

Der Bundesregierung liegen keine Hinweise darauf vor, dass Versicherer aktuell Cloud-Lösungen unternehmens- oder konzernexterner Anbieter (gleich welcher Nationalität des Anbieters) zur Speicherung und Verarbeitung von Daten einsetzen.

Im Bankenbereich wird nach derzeitigem Kenntnisstand von der Auslagerung der Kundendaten per Auslagerungsvertrag in Private Clouds (gegebenenfalls von dritten Service Providern) Gebrauch gemacht. Der Bundesregierung liegen keine Erkenntnisse vor, dass dabei gegen die in der Antwort zu Frage 3 dargelegten Anforderungen verstoßen wird.

21. Falls solche Kenntnisse bestehen, um wie viele und welche Kreditinstitute, Versicherungen und Wertpapierhandelsunternehmen handelt es sich dabei im Einzelnen?

In welchen Staaten befanden oder befinden sich die entsprechenden verbundenen Rechenzentren?

Auf die Antwort zu Frage 20 wird verwiesen.

22. Inwieweit haben die Bundesregierung bzw. deutsche Behörden (z. B. im Wege der Aufsicht) selbst Zugriffsmöglichkeiten auf eine Cloud deutscher Finanzdienstleistungsunternehmen?

Der Zugriff deutscher Behörden auf Einrichtungen oder Daten einer sogenannten Cloud richtet sich nach den Regeln der Sicherstellung/Beschlagnahme und Durchsuchung und ist zu Gefahrenabwehr- und Strafverfolgungszwecken bei Vorliegen der gesetzlichen Voraussetzungen zulässig. Entsprechende Befugnisse lassen sich z. B. in der StPO (§§ 94 ff., 110 StPO) und in den Landespolizeigesetzen sowie dem BKA-Gesetz finden. Ein Zugriff ist nur dann möglich, wenn sich die Technik, auf die zugegriffen werden soll, auf deutschem Hoheitsgebiet befindet. Ein Zugriff der Bundesregierung auf die „Cloud deutscher Finanzdienstleistungsunternehmen“ besteht nicht.

Die BaFin ist im Rahmen der laufenden Aufsicht befugt, von den beaufsichtigten Unternehmen Auskünfte über alle aufsichtsrelevanten Geschäftsangelegenheiten sowie Vorlage oder Übersendung aller Geschäftsunterlagen zu verlangen, siehe etwa § 83 Absatz 1 Satz 1 Nummer 1 des Versicherungsaufsichtsgesetzes; § 25b Absatz 3 Satz 1 i. V. m. § 44 Absatz 1 des Kreditwesengesetzes. Eine eigene Zugriffsmöglichkeit auf eine Cloud der Unternehmen hat die BaFin dabei nicht, die Unterlagen müssen von den unmittelbar beaufsichtigten Unternehmen zur Einsichtnahme zur Verfügung gestellt werden.

23. Welche Daten in einer solchen Cloud können von wem in welcher Detailliertheit und auf welcher Rechtsgrundlage abgefragt werden?

Auf die Antwort zu Frage 22 wird verwiesen.

24. Welche Informationen und Erkenntnisse, insbesondere unter datenschutz- und verbraucherschutzrechtlichen Gesichtspunkten (insbesondere im Zuge des NSA-Skandals), liegen der Bundesregierung bezüglich des Unternehmens IBM als Outsourcingpartner vor, nachdem dieses Unternehmen nach den Rechenzentren der Elektronikmarktkette Media-Saturn-Holding GmbH (seit dem Jahr 2008, vgl. Pressemitteilung vom 10. Dezember 2008 auf www.presseportal.de) auch die zentralen EDV-Strukturen des Versicherungsunternehmens Allianz SE übernehmen soll?

    Inwieweit und in welcher Form bestehen Informationsaustausch und Kontrollmöglichkeiten, auch gemeinsam mit amerikanischen Behörden (bitte aufschlüsseln)?

Sofern die Firma IBM personenbezogene Daten der o. g. Unternehmen verarbeitet, handelt es sich dabei um eine privatrechtliche Auftragsdatenverarbeitung, für die die einschlägigen gesetzlichen Bestimmungen einzuhalten sind. Insofern liegen der Bundesregierung keine Erkenntnisse zur Ausgestaltung und Umsetzung solcher Vertragsverhältnisse vor. Kontrollmöglichkeiten für die Auftragsdatenverarbeitung bestehen für die zuständigen datenschutzrechtlichen Aufsichtsstellen. Hierzu wird auch auf die Antwort zu Frage 8 verwiesen.

Um Verstößen gegen Safe-Harbor-Prinzipien entgegenzuwirken, arbeiten nach entsprechenden Ausführungen auf der Homepage des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die zuständigen Behörden in den USA und die EU-Datenschutzbehörden eng zusammen. Besondere Bedeutung habe dabei auch die Frage, wie die Betroffenen, also Organisationen, Verbraucher und Unternehmensmitarbeiter besser über die sich aus der Vereinbarung ergebenden Rechte unterrichtet werden können.

Gesetzliche Kontrollmöglichkeiten gemeinsam mit amerikanischen Behörden bestehen nicht. Welche vertraglichen Kontrollmöglichkeiten in dem endgültigen Dienstleistungsvertrag für IT-Operations beim Betrieb der Rechenzentren mit IBM vom 20. Dezember 2013 (siehe Pressemitteilung der Allianz im Internet) festgelegt sind, ist nicht bekannt, da derartige Verträge weder einer Genehmigungs- noch Vorlagepflicht unterliegen.

25. Was gedenkt die Bundesregierung im Weiteren zu unternehmen, um Datenschutzverletzungen und Datenmissbrauch durch geheimdienstliche Abschöpfung von Daten deutscher Finanzdienstleistungsunternehmen bzw. der von ihnen beauftragten IT-Dienstleister ggf. aufzudecken und zu verhindern?

Die Bundesregierung hat keine Erkenntnisse, dass Daten deutscher Finanzdienstleistungsunternehmen oder der von Ihnen beauftragten IT-Dienstleister durch Geheimdienste abgeschöpft oder missbraucht werden. Sollten sich konkrete Hinweise auf Datenschutzverletzungen und Datenmissbrauch ergeben, ist es Aufgabe der für den Datenschutz zuständigen Stellen bzw. der Strafverfolgungsbehörden, den Sachverhalt zu ermitteln und die Rechtsverletzungen abzustellen.

26. Ist von Seiten der Bundesregierung diesbezüglich eine konkrete politische Initiative angedacht, und wenn ja, wie sieht diese aus?

Die Bundesregierung klärt die im Zusammenhang mit den Veröffentlichungen auf Basis des Materials von Edward Snowden geäußerten Vorwürfe umfassend auf. Dazu steht sie u. a. in regelmäßigen Kontakt mit britischen und amerikanischen Stellen. Erst nach ausreichender Klärung des Sachverhalts wird die Bundesregierung ggf. erforderliche Maßnahmen einleiten.

Unabhängig davon unterstützt die Bundesregierung geeignete politische Initiativen. So hat vor kurzem die Vollversammlung der Vereinten Nationen eine Resolution zum Schutz der Privatsphäre angenommen, die auf eine Initiative von Deutschland und Brasilien zurückgeht. Deutschland setzt sich weiter dafür ein, dass der Schutz der Bürgerinnen und Bürger bei Drittstaatenübermittlungen deutlich verbessert wird. Dies gilt insbesondere für Safe Harbor. Für Modelle wie Safe Harbor sollte in der neuen europäischen Datenschutz-Grundverordnung ein robuster Rechtsrahmen mit klaren Vorgaben für Garantien der Bürgerinnen und Bürger geschaffen werden. Ziel sollte es insbesondere sein, die Individualrechte der Bürgerinnen und Bürger zu stärken und ihnen bessere Rechtsschutzmöglichkeiten zur Verfügung zu stellen, die Registrierung der US-Unternehmen in der EU vorzunehmen und die staatliche Kontrolle seitens der EU-Datenschutzaufsichtsbehörden in Modellen wie Safe Harbor zu stärken.

27. Wie beurteilt die Bundesregierung Datenschutzverletzungen im Zusammenhang mit dem NSA-Skandal vor dem Hintergrund des Transparenzgebots als Ausfluss des informationellen Selbstbestimmungsrechts der Bürgerin bzw. des Bürgers nach Artikel 2 Absatz 1 des Grundgesetzes (GG) i. V. m. Artikel 1 Absatz 1 GG?

Sofern Datenschutzverletzungen den Tatbestand gesetzlicher Verbote erfüllen bzw. gesetzliche Gebote missachten, ist ein Rückgriff auf das Grundgesetz nicht erforderlich. Verstöße gegen geltendes Recht sind in diesen wie in allen anderen Fällen nicht hinzunehmen.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333