

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Dr. Max Stadler, Ernst Burgbacher, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 16/8578 –**

Standortbestimmung Datenschutz

Vorbemerkung der Fragesteller

Seit einigen Jahren wird von Experten eine Modernisierung des Datenschutzrechts angemahnt. Dafür haben Gutachter bereits in der 14. und 15. Wahlperiode Vorschläge gemacht. Der Innenausschuss des Deutschen Bundestages hat im vergangenen März 2007 zur Modernisierung des Datenschutzes eine Anhörung durchgeführt.

Die voranschreitende technische Entwicklung, die Terrorismusbekämpfung aber auch europäische Regelungen haben Auswirkungen auf den Datenschutz. Private sammeln zudem vermehrt Daten, um sie z. B. für gezielte personalisierte Werbung einzusetzen. Mehrfach hat der Deutsche Bundestag die Bundesregierung aufgefordert ein Datenschutzauditgesetz gemäß § 9a des Bundesdatenschutzgesetzes (BDSG) sowie ein Arbeitnehmerdatenschutzgesetz vorzulegen (zuletzt Bundestagsdrucksache 16/4882).

1. Wie bewertet die Bundesregierung die Entwicklung des Datenschutzrechts in dieser Wahlperiode, insbesondere unter Berücksichtigung europäischer und deutscher Gesetzgebung?

Die Bundesregierung bewertet die Entwicklungen des Datenschutzrechts in dieser Wahlperiode als positiv. Sowohl auf europäischer als auch auf nationaler Ebene wurden datenschutzrechtliche Regelungen an veränderte Lebenssachverhalte angepasst. In einigen Bereichen sind weitere Änderungen noch in dieser Legislaturperiode geplant.

2. Wie bewertet die Bundesregierung die in dieser Wahlperiode beschlossene Weitergabe kommerzieller Daten an staatliche Stellen, wie z. B. Flug- und Passagierdaten zur Terrorismusbekämpfung im Hinblick auf das dem Datenschutzrecht zu Grunde liegende Grundrecht der informationellen Selbstbestimmung?

Das Gesetz zu dem Abkommen vom 26. Juli 2007 zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS) (BGBl. II S. 1978) schafft für den Bereich der PNR-Daten eine Rechtsgrundlage für den transatlantischen Informationsaustausch zur Bekämpfung von Terrorismus und sonstigen schweren Straftaten grenzüberschreitender Art, einschließlich der organisierten Kriminalität. Das Abkommen, welches von den USA lange abgelehnt wurde, dient der Rechtssicherheit. Es enthält bereichsspezifische Regelungen zum Datenschutz.

Sofern nach § 8a Abs. 2 Nr. 1 des Bundesverfassungsschutzgesetzes, der in der gegenwärtig geltenden Fassung durch das Terrorismusbekämpfungsergänzungsgesetz vom 5. Januar 2007 (BGBl. I S. 2) in das Gesetz eingefügt wurde, bei Luftfahrtunternehmen die Namen und Anschriften von Kunden und die Umstände von Transportleistungen erhoben werden können, bestehen keine Bedenken gegen die Wahrung des Verhältnismäßigkeitsprinzips. Die in § 8a Abs. 2 bis 4, 6 und 7 des Bundesverfassungsschutzgesetzes enthaltenen Voraussetzungen und Verfahrensregeln stellen sicher, dass in das informationelle Selbstbestimmungsrecht der Betroffenen nur im Einzelfall hinsichtlich schwerwiegender Gefahren für die in § 3 Abs. 1 des Bundesverfassungsschutzgesetzes genannten Schutzgüter und nur insoweit eingegriffen wird, wie dies jeweils erforderlich ist.

3. Wie bewertet die Bundesregierung die Befürchtung von Datenschützern, dass sich z. B. mit der Einführung der Steuer-Identifikationsnummer die Gefahr der Einführung einer Personenkennziffer erhöht hat?

Bei der steuerlichen Identifikationsnummer nach § 139b der Abgabenordnung (AO IdNr.) handelt es sich nicht um eine Personenkennziffer, sondern um ein bereichsspezifisches Ordnungsmerkmal, welches ausschließlich der eindeutigen Identifizierung des Steuerpflichtigen im Besteuerungsverfahren dient (§ 139b Abs. 2 AO).

Bei Schaffung der gesetzlichen Grundlagen zur IdNr. wurden Regelungen eingeführt, die eine unbefugte Verwendung der IdNr. und der zu ihr gespeicherten Daten verhindern sollen. Danach haben ausschließlich die Finanzbehörden (§ 139b Abs. 4 und 5 AO) Zugriff auf die Daten, die zur jeweiligen IdNr. beim Bundeszentralamt gespeichert sind. Für den Arbeitgeber hält das Bundeszentralamt für Steuern die IdNr., den Tag der Geburt, Merkmale für den Kirchensteuerabzug und folgende Lohnsteuerabzugsmerkmale des Arbeitnehmers zum unentgeltlichen automatisierten Abruf nach amtlich vorgeschriebenen Datensatz bereit (§ 39e EStG). Die Finanzbehörden dürfen diese Daten nur im Rahmen ihrer durch Rechtsvorschrift zugewiesenen Aufgaben verwenden (§ 139b Abs. 4 und 5 AO); die Arbeitgeber dürfen die Daten ausschließlich für die Durchführung des Lohn- und Kirchensteuerabzugs verwenden (§ 39e Abs. 5 Satz 2 EStG). Ein Zugriff sonstiger Stellen auf diese Daten ist ausgeschlossen.

Auch die Verwendung der IdNr. selbst ist gegen Missbräuche gesichert. Die IdNr. ist im Gegensatz zur Rentenversicherungsnummer eine nichtsprechende Nummer (§ 139a Abs. 1 Satz 2 AO). Das heißt, dass aus der Nummer keine Rückschlüsse auf den Steuerpflichtigen gezogen werden können.

Diese Regelungen wurden nicht nur in enger Abstimmung mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) umgesetzt, sondern resultieren zum Teil aus eigenen Vorschlägen des BfDI.

Die Bundesregierung hält daher die Befürchtung von Datenschützern, dass sich mit der Einführung der IdNr. die Gefahr der Einführung einer Personenkennziffer erhöht hat, für unbegründet.

4. Welche Gesetzesvorhaben im Hinblick auf den Datenschutz sind noch für diese Wahlperiode von der Bundesregierung geplant?

Die Bundesregierung strebt an, sowohl einen Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes als auch einen Entwurf eines Datenschutzauditgesetzes so rechtzeitig vorzulegen, dass sie noch in der laufenden Legislaturperiode verabschiedet werden können.

5. Wie wurde der im September 2007 vorgestellte Referentenentwurf zum Datenschutzaudit von den Verbänden bewertet?

Die Verbände lehnen die Einführung eines gesetzlichen Audits aufgrund der Kostenbelastung der Unternehmen und des bürokratischen Mehraufwands ganz überwiegend ab.

6. Wann wird die Bundesregierung voraussichtlich einen Regierungsentwurf zum Datenschutzaudit ins Parlament einbringen?

Siehe Antwort zu Frage 4.

7. Wie wurde der im September 2007 vorgestellte Referentenentwurf zur Änderung des BDSG im Auskunftswesen von den Verbänden bewertet?

Teilweise haben die Verbände noch weitergehende, d. h. die betroffenen Unternehmen weiter einschränkende Regelungen gefordert, teilweise wurden die geplanten Regelungen als zu weitgehend abgelehnt.

8. Wann wird die Bundesregierung voraussichtlich einen Regierungsentwurf zur Änderung des BDSG im Auskunftswesen ins Parlament einbringen?

Siehe Antwort zu Frage 4.

9. Mit welchen Maßnahmen unterstützt die Bundesregierung das Zustandekommen einer Selbstverpflichtungserklärung der Wirtschaft zum Einsatz von RFID-Chips?

Die Bundesregierung beobachtet seit Jahren aufmerksam die datenschutzrelevanten Entwicklungen im Bereich Radio Frequency Identification (RFID) und steht mit den betroffenen Kreisen in Wirtschaft, Daten- und Verbraucherschutz in regelmäßigem Dialog.

Zudem hat die Bundesregierung in ihrem jüngsten „Bericht zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie“ (Bundestagsdrucksache 16/7891 vom 23. Januar 2008) empfohlen, zunächst

auf gesetzgeberische Maßnahmen zu verzichten und stattdessen einer Selbstverpflichtung der Wirtschaft den Vorzug zu geben.

10. Warum kommt die Bundesregierung zur der Erkenntnis, dass die Industrie sich in der Frage der Selbstregulierung hinsichtlich des Einsatzes von RFID-Chips „problembewusst gezeigt habe“, wenn die bisherigen Vorschläge keine ausreichenden Mindeststandards zum Schutz der Privatsphäre und Sanktionsmechanismen vorsehen (siehe Meldung auf Heise-Online vom 13. Februar 2008, Bundesregierung hält Big-Brother-Szenarien bei RFID für weit hergeholt)?

Kaum eine andere Technologie hat in den betroffenen Wirtschaftskreisen bereits so weit im Vorfeld flächendeckender Anwendung ähnlich große Informations- und Diskussionsbereitschaft ausgelöst wie RFID. Zu den diesbezüglichen Aktivitäten der Wirtschaft zählen Verbraucherinformationsforen ebenso wie die regelmäßige Teilnahme an Arbeitskreisen, Workshops und bilateralen Gesprächen (u. a. auch mit dem Bundesministerium des Innern (BMI) und dem Bundesministerium für Wirtschaft und Technologie (BMWi)); siehe hierzu im Übrigen den „Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie“ (Bundestagsdrucksache 16/7891 vom 23. Januar 2008, S. 11).

11. Welche besonderen Kampagnen plant die Bundesregierung noch für diese Wahlperiode, um den Bekanntheitsgrad von datenschutzrelevanten Themen – wie z. B. RFID – zu erhöhen?

Die Bundesregierung plant derzeit keine besonderen Kampagnen.

12. Werden bei Ausschreibungen des Bundes auch datenschutzrechtliche Ausschreibungskriterien, z. B. Einsatz datenschutzrechtlicher Technologie, gefordert?

Von Bundesbehörden ausgeschriebene Leistungen müssen dem geltenden Recht entsprechen. Dazu gehört ggf. auch die Beachtung der einschlägigen datenschutzrechtlichen Anforderungen. Zum Teil werden in Ausschreibungen auch ausdrücklich Anforderungen an den Schutz personenbezogener Daten gestellt, die auf die Beschaffung datenschutzgerechter Technologien abzielen.

13. Werden datenschutzfreundliche Techniken gezielt von der Bundesregierung gefördert, und wenn ja, welche, und in welcher Höhe?

Die Bundesregierung fördert in zahlreichen Projekten gezielt den Einsatz oder die Entwicklung datenschutzfreundlicher Technologien.

Das unter Federführung des BMI stehende Projekt Bürgerportale soll das Versenden und Empfangen von Nachrichten und Dokumenten im Internet so einfach, sicher, vertraulich und verbindlich machen wie heute die Papierpost. Dafür soll ein Verbund von staatlich zertifizierten, aber privat betriebenen Anbietern von sicheren E-Mail-Diensten aufgebaut werden. Die Zertifizierung soll neben Funktionalität, IT-Sicherheit und Verbraucherschutz auch den Datenschutz umfassen.

Das Projekt ist Teil der Hightechstrategie und des E-Government-Programms 2.0 der Bundesregierung sowie des 12-Punkteplans für ein bürgerfreundliches Deutschland.

Mit dem elektronischen Personalausweis (ePA) soll künftig der elektronische Identitätsnachweis (eID-Nachweis) im Internet und gegenüber Automaten ermöglicht werden. Diese – für den Bürger fakultative – Bürgerkartenfunktion wird den Datenschutz nicht nur normativ, sondern auch technisch unterstützen. Den technischen Lösungen des elektronischen Personalausweises liegen international im Rahmen der Internationalen Zivilluftfahrt-Organisation (ICAO) bzw. im Rahmen der EU abgestimmte Kryptographieverfahren zugrunde.

Die Bereitstellung der Personendaten beim elektronischen ID-Nachweis mit dem elektronischen Personalausweis soll dabei immer ein bewusstes Handeln des Personalausweisinhabers erfordern und so seine informationelle Selbstbestimmung stärken. Der Personalausweisinhaber wird zusätzlich zur Bereitstellung seines elektronischen Personalausweises mit einem Kartenleser die nur ihm bekannte PIN eingeben müssen, dabei das Zertifikat des Diensteanbieters überprüfen können und im Einzelfall über die Auswahl der vom Chip auszulésenden Personendaten entscheiden können. Die Ausstellungsgebühr für ePA und die Kosten für die Anwendung, Kartenleser etc. trägt grundsätzlich der anwendende PA-Inhaber.

Der Internet-Diensteanbieter oder Automatenbetreiber wird von Amts wegen ein Zertifikat (Zugriffsschlüssel) erhalten und nur mit diesem auf die zweckgebunden ausgewählten Personendaten im elektronischen Ausweis zugreifen können. Bei der Erteilung der widerrufbaren Zertifikate soll eine Prüfung der Erforderlichkeit von Personendaten für den Geschäftszweck des Diensteanbieters erfolgen. So wird das Missbrauchspotential eingeschränkt und die Verwendung der Daten offen gelegt und nachvollziehbar. Identitätsdiebstahl bspw. durch das rasant ansteigende „Phishing“ wird weitgehend ausgeschlossen. Die Gebühren der Zertifikate für die Diensteanbieter, sollen zur Aufwandsdeckung herangezogen werden.

Vorarbeiten für die Einführung des ePA und zum Identitätsmanagement werden im Rahmen der Hightechstrategie der Bundesregierung gefördert.

Die Virtuelle Poststelle (VPS) unterstützt insbesondere die Verwendung des Transportprotokolls Online Services Computer Interface (OSCI-Transport 1.2), das maßgeblich im E-Government als Standard für die elektronische Kommunikation zum Einsatz kommt. Die Datenschutzbeauftragten des Bundes und der Länder (siehe Beschluss der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 29. Oktober 2004) empfehlen den Einsatz von OSCI-Transport für die datenschutzgerechte Ende-zu-Ende-Sicherheit im E-Government, da dieses eine durchgehende Sicherheit vom Versand bis zum Empfang einer Datenübermittlung gewährleistet. Die VPS leistet somit einen wesentlichen Beitrag zum praktischen Einsatz datenschutzfreundlicher Technik.

Daneben sind zahlreiche Projekte zur Erhöhung der Sicherheit und Vertraulichkeit in der E-Mail-Kommunikation zu nennen (z. B. Gpg2, Ägypten/Kleopatra, Kolab/Kontakt, Gpg4win etc.), die durch den Einsatz kryptographischer Verschlüsselung und Signaturen die Voraussetzung für Vertraulichkeit, Authentizität und Integrität in der E-Mail-Kommunikation schaffen. Durch den Schutz vor unerlaubter Einsicht und Manipulation wird der Datenschutz unmittelbar gestärkt.

Das Bundesamt für Sicherheit in der Informationstechnik hat den Europäischen Datenschutzbeauftragten im Rahmen des EURODAC-Audits unterstützt. Das Audit erfolgte nach ISO 27001 auf der Basis von IT-Grundschutz.

14. Wie bewertet die Bundesregierung die bisherigen Regelungen für Pseudonymisierungskonzepte, und welchen Änderungsbedarf sieht sie?

Die bestehenden Regelungen für Pseudonymisierungskonzepte haben sich bisher bewährt. Gegenwärtig wird kein Änderungsbedarf gesehen.

Im Technologieprojekt „AN.ON – Anonymität.Online“ hat das BMWi darüber hinaus die Entwicklung leistungsfähiger Protokolle und Architekturen zur anonymen und unbeobachtbaren Bewegung eines Nutzers im Internet gefördert, die auf den bestehenden rechtlichen Regelungen aufsetzen (www.datenschutz-zentrum.de/projekte/anon/index.htm#einf).

15. Wie bewertet die Bundesregierung die verbandliche Selbstregulierung im Bereich des Datenschutzes?
16. Wird das vorgesehene Instrument des Aufstellens von Verhaltensregeln durch Verbände gemäß § 38a BDSG ausgiebig genutzt, und wenn nein, welche Ursachen gibt es dafür?

Verbände können jederzeit und unabhängig von § 38a BDSG für ihre Mitglieder Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen aufstellen. § 38a BDSG gewährleistet, dass die Entwürfe für derartige Verhaltensregeln der Aufsichtsbehörde unterbreitet werden, und verpflichtet diese, die Vereinbarkeit mit dem geltenden Datenschutzrecht zu überprüfen. Die Überprüfung erfolgt auf Länderebene durch die zuständige Aufsichtsbehörde nach § 38 Abs. 6 BDSG i. V. m. dem Landesrecht. Der Bundesregierung liegen keine näheren Erkenntnisse vor, in welchem Umfang Verbände von der Möglichkeit des § 38a BDSG Gebrauch machen.

17. Hält die Bundesregierung das bestehende Sanktionensystem hinsichtlich der genannten Tatbestände, der Höhe der Bußgelder bzw. der Strafandrohung, dem Antragserfordernis gemäß § 44 BDSG und der tatsächliche verhängten Sanktionen im BDSG für ausreichend und angemessen, und wenn nein, welche Gegenmaßnahmen wird die Bundesregierung ergreifen?

Das bestehende Sanktionssystem der §§ 43, 44 BDSG, das durch bereichsspezifische Straf- und Bußgeldvorschriften ergänzt wird, hat sich nach Auffassung der Bundesregierung grundsätzlich als ausreichend und angemessen bewährt. Zum verbesserten Schutz der Rechte der Betroffenen plant die Bundesregierung die Einführung eines neuen Bußgeldtatbestands für den Fall, dass der Auskunftsanspruch des Betroffenen nach § 34 BDSG nicht ordnungsgemäß erfüllt wird.

18. Wie bewertet die Bundesregierung die Wirksamkeit der unterschiedlichen Zuständigkeiten der Aufsichtsbehörden für den öffentlichen und nicht-öffentlichen Bereich für ein und dieselbe Branche (z. B. Verkehrsbetrieb, Energieversorgung, Sport- und Freizeitveranstaltungen) je nach Rechtskonstruktion?

Die Regelung der angesprochenen Zuständigkeitsfragen liegt in der Kompetenz der Länder und ist daher einer Bewertung durch die Bundesregierung entzogen.

19. Welche Formen der Kooperation und Abstimmung gibt es zwischen den Aufsichtsbehörden für Datenschutz auf nationaler und europäischer Ebene?

Die Aufsichtsbehörden i. S. d. § 38 BDSG treffen sich halbjährlich im sog. Düsseldorfer Kreis und auf europäischer Ebene in der sog. Artikel-29-Gruppe sowie der Europäischen Datenschutzkonferenz.

20. Hält die Bundesregierung die bisherigen Befugnisse der Aufsichtsbehörde, insbesondere bei einer widerrechtlichen Verarbeitung von personenbezogenen Daten, für ausreichend, und wie begründet sie das?

Die bestehenden Befugnisse der Aufsichtsbehörden nach § 24 ff., § 38 BDSG sowie den jeweiligen Datenschutzgesetzen der Länder haben sich nach Auffassung der Bundesregierung als ausreichend und angemessen bewährt, die widerrechtliche Verarbeitung personenbezogener Daten festzustellen und zu unterbinden. Der Bundesregierung sind keine Fälle bekannt, in denen eine Aufsichtsbehörde mangels Befugnis nicht ausreichend auf einen Verstoß gegen datenschutzrechtliche Vorschriften reagieren konnte. Die Bundesregierung sieht daher derzeit keinen Handlungsbedarf.

21. Ist der Bundesregierung bekannt, in wie vielen Fällen die Mitteilung der Datenschutzaufsichtsbehörde gegenüber der Gewerbeaufsichtsbehörde gemäß § 38 Abs. 1 Satz 5 BDSG zu gewerberechtlichen Maßnahmen geführt und dieses Instrument praktische Bedeutung erlangt hat?

Nein, der Bundesregierung ist keine Fallzahl bekannt.

22. Nach welchen objektiven Kriterien stellen die Aufsichtsbehörden nach §§ 24, 25 und 38 Abs. 5 BDSG sowie § 115 Abs. 4 TKG eine nicht ausreichende Fachkunde und Zuverlässigkeit fest?

Der Bundesregierung liegen keine Erkenntnisse vor, nach welchen Kriterien die Datenschutz-Aufsichtsbehörden der Länder nach § 38 Abs. 5 BDSG eine nicht ausreichende Fachkunde und Zuverlässigkeit feststellen.

Soweit der BfDI im TK-Bereich datenschutzrechtliche Aufsichtsbehörde ist, weist er darauf hin, dass kein formaler Kriterienkanon für die Feststellung der Fachkunde und Zuverlässigkeit betrieblicher Datenschutzbeauftragter bei TK-Unternehmen besteht. Fachkunde setzt hier entsprechend der allgemeinen Interpretation der gesetzlichen Vorgaben die sichere Kenntnis der datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes und des Bundesdatenschutzgesetzes sowie gute Kenntnisse der betrieblichen IT voraus. Bei der Zuverlässigkeit geht es neben der persönlichen Eignung insbesondere auch um die Kompatibilität mit anderen Aufgaben.

23. Wie viele Unternehmen wurden in den letzten fünf Jahren nach § 115 Abs. 4 TKG wegen fehlender oder unzureichend qualifizierter betrieblicher Datenschutzbeauftragter vom BfDI gerügt oder wegen einer Ordnungswidrigkeit belangt?

Der BfDI hat hierzu Folgendes mitgeteilt:

Sofern sich anlässlich der Stellungnahmen betrieblicher Datenschutzbeauftragter zu datenschutzrechtlichen Eingaben von Kunden Defizite hinsichtlich der Qualifikation oder der datenschutzrechtlichen Sensibilisierung zeigen, wirkt der BfDI auf eine bessere Aus- und Fortbildung der betrieblichen Datenschutzbeauftragten, ihrer Mitarbeiter und der in der automatisierten Datenverarbeitung der TK-Unternehmen tätigen Mitarbeiter hin. Die unzureichende Beantwortung von Anfragen des BfDI hat in den letzten Jahren wiederholt zu Beratungs- und Kontrollbesuchen geführt. Eine förmliche Sanktion wegen unzureichender Ausbildung oder Qualifikation betrieblicher Datenschutzbeauftragter im Sinne einer Beanstandung (§ 25 BDSG) ist zumindest in den letzten fünf Jahren nicht erfolgt.

24. Welche datenschutzrechtlichen Probleme ergeben sich bei der europäischen und internationalen Zusammenarbeit im Hinblick auf die unterschiedlichen Datenschutzniveaus?

Keine datenschutzrechtlichen Probleme ergeben sich bei der Übermittlung personenbezogener Daten an Stellen in anderen Mitgliedstaaten der Europäischen Union, in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder der Organe und Einrichtungen der Europäischen Gemeinschaften, soweit Tätigkeiten betroffen sind, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen. Hier gelten im Wesentlichen dieselben Regelungen wie für die Übermittlung personenbezogener Daten an inländische Stellen (§ 4b Abs. 1 BDSG). Ein angemessenes Datenschutzniveau ist in diesen Fällen über die EG-Datenschutzrichtlinie 95/46/EG gewährleistet.

Erfolgt die Datenweitergabe dagegen an sonstige ausländische, über- oder zwischenstaatliche Stellen oder fällt sie nicht ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften, muss die Übermittlung unterbleiben, soweit der Betroffene ein schutzwürdiges Interesse an deren Ausschluss hat. Davon ist insbesondere dann auszugehen, wenn auf Seiten der Empfänger kein angemessenes Datenschutzniveau gewährleistet ist (§ 4b Abs. 2 Satz 1 und 2 BDSG). Eine Datenübermittlung ist in diesem Falle nur möglich, wenn einer der Ausnahmetatbestände des § 4b Abs. 2 Satz 3 oder des § 4c BDSG erfüllt ist.

Im November 2007 hat sich zudem der Rat der Europäischen Union politisch auf einen Rahmenbeschluss zum Datenschutz in der 3. Säule geeinigt.

25. Wie wird sichergestellt, dass der Empfängerstaat mit den übermittelten personenbezogenen Daten ordnungsgemäß umgeht?

Vor Übermittlung der Daten hat die verantwortliche Stelle zu prüfen, ob und inwieweit der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat, insbesondere ob bei der empfangenden Stelle ein angemessenes Datenschutzniveau gewährleistet ist (§ 4b Abs. 2 BDSG).

Die Angemessenheit des Schutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunftsland und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Landesregeln und Sicherheitsmaßnahmen herangezogen werden (§ 4b Abs. 3 BDSG).

Ergibt die Prüfung, dass ein angemessenes Datenschutzniveau nicht gewährleistet ist, unterbleibt die Übermittlung, es sei denn die unter Frage 24 genannten Ausnahmetatbestände liegen vor. Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle (§ 4b Abs. 5 BDSG).

Sieht ein internationales Abkommen die Übermittlung personenbezogener Daten ins Ausland vor, wirkt die Bundesregierung zudem regelmäßig darauf hin, dass in den Vertragstext eine detaillierte Datenschutzklausel aufgenommen wird.

In jedem Falle ist die Stelle, an die die Daten übermittelt werden, auf den Zweck hinzuweisen, zu dessen Erfüllung die Übermittlung erfolgt (§ 4b Abs. 6 BDSG).