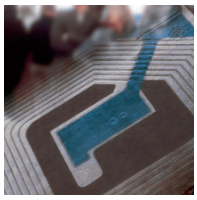
Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit



# Tätigkeitsbericht zum Datenschutz für die Jahre 2009 und 2010

23. Tätigkeitsbericht

# Tätigkeitsbericht 2009-2010

23. Tätigkeitsbericht

Dieser Bericht wurde am 12. April 2011 dem Präsidenten des Deutschen Bundestages, Herrn Dr. Norbert Lammert, überreicht.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Peter Schaar

# Unterrichtung

## durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

## Tätigkeitsbericht 2009 und 2010 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – 23. Tätigkeitsbericht –

Inhaltsverzeichnis




*Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 12. April 2011 gemäß § 26 Absatz 1 des Bundesdatenschutzgesetzes.*

Im Tätigkeitsbericht sind nur die Entschließungen abgedruckt, auf die in den Beiträgen unmittelbar Bezug genommen wird. Alle Entschließungen der Datenschutzkonferenzen und weitere Informationen finden Sie auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter www.datenschutz.bund.de

Seite

Seite

Seite

Seite

Seite

## Einführung

Das Interesse an datenschutzrechtlichen Themen nimmt weiter zu, was sich nicht allein an der vielfältigen Berichterstattung der Medien festmachen lässt, sondern auch an den weiterhin zunehmenden Zahlen der Beschwerden und Fragen von Bürgerinnen und Bürgern, die mich erreichen. So trafen im Jahr 2010 fast dreimal so viele Eingaben von Bürgerinnen und Bürgern bei meiner Dienststelle ein als fünf Jahre zuvor.

Dies signalisiert einerseits, dass die objektiven Herausforderungen an den Datenschutz weiter zugenommen haben. Zugleich zeigt sich aber, dass den Menschen die Wahrung ihrer Privatsphäre wichtig ist.

Besonders deutlich wurde das wachsende Interesse in der Diskussion über Google Street View. Überraschend viele Menschen legten Widerspruch gegen die Veröffentlichung von Bildern ihrer Häuser und Grundstücke ein, ehe der Dienst überhaupt seinen Betrieb aufgenommen hatte. Aber auch die Debatte über staatliche Eingriffe in den Datenschutz setzt sich fort – etwa über die Vorratsdatenspeicherung, über den Zugriff von US-Behörden auf europäische Finanzdaten oder über den Einsatz von „Körperscannern“ an Flughäfen.

Innovationen, die in den letzten zehn Jahren auf verschiedenen Feldern entwickelt wurden – Ortungssysteme, Internet, digitale Videotechnik, Mustererkennung, RFID – werden kombiniert und finden in rasender Geschwindigkeit Eingang in den Alltag von immer mehr Menschen. Alte Geschäftsmodelle erfahren einen elektronischen Qualitätssprung, etwa die gezielte Vermarktung von Produkten. Neue Dienste entstehen und werden millionenfach genutzt, etwa die sozialen Netzwerke im Internet, die längst ihren Sprung aus einem universitären Umfeld in den beruflichen und privaten Alltag geschafft haben. „Smarte“ Technologien, etwa zur Messung und Steuerung der Energieversorgung, werden eingeführt und es ist noch nicht entschieden, ob dies letztlich zu mehr individueller Freiheit oder zu mehr Überwachung führt.Wie ambivalent die neuen Techniken sind, wird weltweit auch an der Nutzung elektronischer Kommunikationsmittel und sozialer Netzwerke in den politischen Debatten und Auseinandersetzungen deutlich: Zum einen gestatten sie eine leichte Kontaktaufnahme, freie Diskussionen und Verabredungen. Zum anderen werden sie von autoritären Regierungen zur Kontrolle und Verfolgung der Teilnehmenden genutzt. Die Möglichkeit zur Veröffentlichung riesiger Datenmengen im Internet per Mausklick (etwa durch WikiLeaks) kann für mehr Transparenz sorgen. Sie kann aber auch dazu führen, dass sensibelste – auch persönliche – Daten in Umlauf geraten und kaum noch rückholbar sind. Nutzen und Risiken treten hier in besonderer Weise zu Tage.Wenn man bedenkt, dass das derzeitige Datenschutzrecht in der „offline-Welt“ des 20. Jahrhunderts entstand und in seinen Grundzügen bereits vor 30 Jahren formuliert wurde, kann es nicht verwundern, dass es den technologischen Herausforderungen nicht mehr angemessen Rechnung trägt. Aus diesem Grund haben die Datenschutzbeauftragten des Bundes und der Länder unter meiner Federführung „Eckpunkte für ein modernes Datenschutzrecht im 21. Jahrhundert“ formuliert, die hoffentlich bei der überfälligen Modernisierung des Datenschutzrechts berücksichtigt werden. Ein herausragendes Ereignis dieser Berichtsperiode war das Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung. Mit erfreulich deutlichen Worten hat das Gericht klargestellt, dass eine totale Überwachung der Bürgerinnen und Bürger mit der verfassungsrechtlichen Identität der Bundesrepublik Deutschland nicht vereinbar wäre. Auch wenn das Gericht nicht jegliche Vorratsdatenspeicherung a priori als unzulässig bewertet, hat es doch das vom Bundestag in der 16. Legislaturperiode beschlossene Gesetz für verfassungswidrig und nichtig erklärt. Ob die Vorratsdatenspeicherung erneut in Deutschland eingeführt wird, hängt nicht zuletzt von Entwicklungen auf europäischer Ebene ab, insbesondere vom Ergebnis der Überprüfung der entsprechenden EG-Richtlinie. Überhaupt sind den Möglichkeiten, den Datenschutz durch nationales Recht effektiv zu gewährleisten, immer engere Grenzen gesetzt. Der zunehmende internationale Datenverkehr, die ständige Verfügbarkeit des Internets und die rasante Verbreitung „intelligenter“ mobiler Endgeräte unterstreichen die Notwendigkeit, auf internationaler Ebene zu akzeptierten Standards für die Sicherung der Privatsphäre zu gelangen. Dabei kommt der Weiterentwicklung des EU-Rechtsrahmens für den Datenschutz große Bedeutung zu. Mit dem Inkrafttreten des Vertrags von Lissabon ist der

Datenschutz zu einem einklagbaren europäischen Grundrecht aufgewertet worden. Die bisherige „Säulenstruktur“ der EU wurde durch eine übergreifende Ordnung ersetzt, die sowohl den Binnenmarkt als auch die polizeiliche und justizielle Zusammenarbeit umfasst. Deshalb wirke ich intensiv an den Diskussionen über die Ausgestaltung des neuen europaweiten Datenschutzrechts mit. So ist das erwähnte „Eckpunktepapier“ der deutschen Datenschutzkonferenz auch ein Beitrag zu einem europaweit internetfähigen Datenschutzrecht. Einerseits muss der neue EU-Rechtsrahmen den Risiken der neuen Techniken angemessen Rechnung tragen, andererseits sollten technologische Möglichkeiten entwickelt und eingesetzt werden, um personenbezogene Daten besser zu schützen. Technologischer Datenschutz beschränkt sich insofern nicht auf eine datenschutzmäßige „Gefahrenabwehr“ – etwa gegen die heimliche Bildung von Persönlichkeitsprofilen –, sondern sollte auch als Chance verstanden werden, den Bürgerinnen und Bürgern die Kontrolle über ihre Daten zurückzugeben. Recht und Technik wirken beim Datenschutz eng zusammen – dies zieht sich wie ein roter Faden durch den gesamten vorliegenden Bericht. Es kann dabei nicht der Anspruch des Rechts sein, jede einzelne technologische Entwicklung im Detail nachzubilden und jeweils detaillierte Schutzvorkehrungen zu definieren. Vielmehr müssen die wesentlichen technischen Vorgaben in neutraler Form formuliert werden, so dass sie bei neuen Verfahren und technologischen Entwicklungen angemessen umgesetzt werden können. Datenschutz ist dabei stets auch der Versuch, einen Ausgleich zwischen den Segnungen der Technik und dem Recht des einzelnen auf Wahrnehmung seines Grundrechts auf informationelle Selbstbestimmung zu finden.

Der Datenschutz als gesellschaftliches Anliegen hängt in besonderer Weise von einer breiten Unterstützung ab, die ich auch in den letzten beiden Jahren in meiner Arbeit erfahren habe. Mein Dank gilt den Abgeordneten des Deutschen Bundestages aller Fraktionen, aber auch allen anderen Vertretern öffentlicher und privater Stellen, die sich für den Datenschutz interessiert und eingesetzt haben. Aber auch dort, wo Meinungsgegensätze und unterschiedliche Positionen bestehen, habe ich Respekt für meine Aufgaben und meine Auffassungen erfahren. Auch dafür danke ich. Besonders möchte ich meinen Mitarbeiterinnen und Mitarbeitern danken, ohne deren Fachwissen, Engagement und Kreativität meine Arbeit so nicht möglich gewesen wäre, zumal sie dabei häufig unter den Grenzen knapper Ressourcen zu leiden hatten.

Auch wenn die Personalausstattung meiner Dienststelle im Berichtszeitraum das erste Mal seit meiner Amtsaufnahme 2003 spürbar verbessert wurde, haben zugleich die Aufgaben und damit auch die Anforderungen an die Mitarbeiterinnen und Mitarbeiter deutlich zugenommen. So wurde mir durch Gesetz die Schlüsselverwaltung für das wohl größte Datenschutzprojekt im Sozialwesen, das Datenbanksystem ELENA übertragen. Außerdem bin ich ab dem 1. Januar 2011 für die datenschutzrechtliche Kontrolle der Jobcenter zuständig, die bisher den Landesdatenschutzbeauftragten oblag. Schließlich ergeben sich durch die Ausweitung der grenzüberschreitenden Datenverarbeitung (etwa im Rahmen von Europol, Schengen und beim Binnenmarktinformationssystem IMI) zusätzliche Herausforderungen mit erheblicher Ressourcenbindung. Da absehbar ist, dass sich der Aufgabenzuwachs fortsetzen wird, halte ich die weitere Verbesserung der personellen Ausstattung meiner Dienststelle für erforderlich.

Peter Schaar

## Zusammenfassung aller Empfehlungen

Ich empfehle dem Gesetzgeber, das Eckpunktepapier der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Modernisierung des Datenschutzrechts bei der überfälligen grundlegenden Neukonzeption des Datenschutzrechts zu berücksichtigen (Nr. 1.1/1.2).

Technische und rechtliche Lösungen können den Datenschutz internetfähig machen. Dazu gehört auch das Löschen von personenbezogenen Daten. Der Gesetzgeber ist hier gefragt. (Nr. 1.6).

Das Urteil des EuGH zur Unabhängigkeit der Datenschutzaufsicht muss auch für den BfDI umgesetzt werden. Für seine Aufsichtstätigkeit bei Post- und Telekommunikationsdienstleistern benötigt der BfDI die erforderlichen Durchsetzungsbefugnisse, insbesondere zur Verfolgung von Ordnungswidrigkeiten (Nr. 2.1).

Die gesetzlichen Benachrichtigungspflichten der Betroffenen sollten durch den Gesetzgeber verbessert werden (Nr. 2.6).

Ein selbstbestimmtes Identitätsmanagement kann die Bürgerinnen und Bürger vor Identitätsdiebstahl und Profilbildung schützen. Der Staat sollte die rechtlichen und technischen Voraussetzungen hierfür schaffen (Nr. 3).

Berechtigungszertifikate zur elektronischen Identifikation mit dem neuen Personalausweis sollten nur an solche Diensteanbieter vergeben werden, die ein ausreichendes Datenschutz- und Datensicherheitsniveau nachweisen (Nr. 3.2).

Die Finanzverwaltung sollte den Steuerpflichtigen die Möglichkeit eröffnen, ihre Kommunikation durch eine qualifizierte elektronische Signatur (qeS) abzusichern. Soweit andere Identifikationsverfahren zum Einsatz kommen sollen, müssen sie mindestens das Sicherheitsniveau der qeS gewährleisten (Nr. 3.6).

Der Gesetzgeber sollte den Betroffenen ein Widerspruchsrecht gegen Internetveröffentlichungen einräumen. Ein bei einer vertrauenswürdigen Stelle eingerichtetes Widerspruchsregister kann die datenschutzfreundliche Inanspruchnahme des Widerspruchsrechts gewährleisten (Nr. 4.1/4.2).

Ich empfehle den gesetzlichen Krankenkassen und anderen meiner Datenschutzkontrolle unterstehenden Stellen, den Einsatz von nicht datenschutzgerechten Systemen zur Reichweitenmessung bei Online-Angeboten umgehend einzustellen und die vorhandenen Daten zu löschen (Nr. 4.3.1).

Ich empfehle der Bundesregierung, eine Änderung des Telemediengesetzes, um eine Einwilligungslösung für das Setzen von cookies und anderen Techniken zur Verfolgung des Nutzerverhaltens im Internet zu normieren (Nr. 4.4).

Ich empfehle dem Gesetzgeber, eine ausdrückliche Rechtsgrundlage für die Veröffentlichung von Wahlvorschlägen im Internet zu schaffen (Nr. 4.10).

Ich empfehle den öffentlichen Stellen, die in der Nationalen E-Government-Strategie definierten Ziele Datenschutz und Informationsfreiheit und damit die Idee des Open Government mit Leben zu erfüllen (Nr. 5).

Ich empfehle dem Gesetzgeber, bei der Novellierung des Energiewirtschaftsgesetzes angemessene Datenschutzregelungen für die Nutzung der neuen intelligenten Stromzähler vorzusehen, damit der gläserne Stromkunde vermieden wird (Nr. 5.1).

Ich empfehle der Bundesverwaltung und den meiner Datenschutzkontrolle unterliegenden sonstigen Stellen, das Einscannen von Personalaktendaten manipulationssicher und datenschutzgerecht zu organisieren und nur durch Beschäftigte der Personalabteilung durchführen zu lassen. Die Integrität der eingescannten Dokumente sollten durch eine qualifizierte digitale Signatur geschützt werden (Nr. 5.5 und 12.3).

Ich empfehle der Bundesverwaltung und den meiner Datenschutzkontrolle unterliegenden sonstigen Stellen, Dienstleitungen über Cloud Computing nur dann zu realisieren, wenn der Datenschutz rechtlich, technisch und organisatorisch sichergestellt wird. Voraussetzungen sind insbesondere gesicherte gesetzliche Grundlagen für den Datenschutz und eine unabhängige Datenschutzkontrolle. Sensible Daten dürfen auch

beim Cloud Computing grundsätzlich nicht außerhalb des EWR verarbeitet werden (Nr. 5.6).

Ich empfehle der Bundesregierung, für die bei den Sicherheitsbehörden des Bundes betriebenen Datenbanken Systeme vorzusehen, die zum Zwecke der Datenschutzkontrolle eine Protokollierung aller Transaktionen gewährleisten (Nr. 5.7 und 7.1.3).

Ich empfehle der Bundesregierung, anstelle der anlasslosen Vorratsdatenspeicherung die Einführung des Quick-Freeze-Verfahrens (Nr. 6.1).

Ich empfehle der Bundesregierung, die anstehenden Evaluierungen der Sicherheitsgesetze auf der Grundlage eines umfassenden Bewertungsansatzes durch eine unabhängige Stelle nach wissenschaftlichen Kriterien durchführen zu lassen(Nr. 7.1.1).

Ich empfehle dem Gesetzgeber, Befugnisse zur polizeilichen Recherche im Internet, deren Inhalt und Grenzen spezialgesetzlich zu regeln (Nr. 7.1.7).

Ich empfehle dem Deutschen Bundestag, die Beteiligung der Sicherheitsbehörden an Zuverlässigkeitsüberprüfungen im Rahmen von Akkreditierungsverfahren bei Großveranstaltungen auf eine gesetzliche Grundlage zu stellen (Nr. 7.2.3).

Ich empfehle der Bundesregierung, einen regelhaften Einsatz von Körperscannern auf deutschen Flughäfen erst dann vorzunehmen, wenn der derzeit durchgeführte Versuch den Nachweis eines Sicherheitsgewinns und der Einsatztauglichkeit derartiger Geräte erbracht hat und der Schutz der Persönlichkeitsrechte gewährleistet ist. Zudem sollte sich die Bundesregierung auf europäischer Ebene für einen hohen Mindeststandard beim Einsatz von Körperscannern einsetzen (Nr. 7.3.1).

Ich empfehle der Bundesregierung, den beabsichtigten Ausbau des nachrichtendienstlichen Informationssystems NADIS zu einem umfassenden Wissensnetz bis zur Schaffung einer entsprechenden Gesetzesänderung auszusetzen (Nr. 7.5.1).

Ich erwarte von der Bundesregierung, dass sie bei der Durchführung des Zensus 2011 die Einhaltung der gesetzlichen Zweckbindungsregelungen sicher stellt, auf die frühestmögliche Datenlöschung achtet sowie für eine hohe Datensicherheit sorgt (Nr. 8.1.1).

Ich empfehle dem Gesetzgeber, die europarechtlichen Vorgaben zum Schutz personenbezogener Daten von Unionsbürgern auch bei einer Speicherung dieser Daten im Ausländerzentralregister vollumfänglich umzusetzen (Nr. 8.2.1).

Ich empfehle dem Gesetzgeber, im Errichtungsgesetz für ein Nationales Waffenregister den Vorkehrungen zum Persönlichkeitsschutz einen hohen Stellenwert einzuräumen und die erforderlichen datenschutzrelevanten Regelungen zu treffen (Nr. 8.3).

Ich empfehle dem Gesetzgeber, die gesetzlichen Grundlagen für das Register der Entscheidungen in Staatsangehörigkeitsangelegenheiten (EStA) über die derzeitigen Bestimmungen des § 33 StAG hinaus im erforderlichen Umfang zu konkretisieren (Nr. 8.4).

Ich empfehle dem Gesetzgeber, Regelungslücken zur Auftragsdatenverarbeitung im StUG analog § 11 BDSG zu schließen (Nr. 8.5.3).

Ich empfehle dem Gesetzgeber, sämtliche zeugnisverweigerungsberechtigten Berufsgeheimnisträger in den absoluten Schutz des § 160a Absatz 1 StPO einzubeziehen (Nr. 8.10).

Ich empfehle dem Gesetzgeber, konkrete Regelungen zum Umgang mit Angeboten von Daten zu Steuersachverhalten zu schaffen, die aus illegalen Quellen stammen. Damit würden die rechtlichen Rahmenbedingungen für behördliche Ermittlungshandlungen vorgegeben und die betroffenen widerstreitenden Interessen in einen angemessenen Ausgleich gebracht werden können (Nr. 9.1).

Ich empfehle dem Gesetzgeber, Regelungen im Zusammenhang mit der Erhebung und Verarbeitung der Steuer-Identifikationsnummer durch nicht-öffentliche Stellen so auszugestalten, dass Steuerpflichtige der Erhebung und Verwendung widersprechen

können und ihnen dabei auch alternative Formen des Nachweises über die relevanten steuerlichen Sachverhalte gegenüber der Finanzverwaltung offen stehen (Nr. 9.2).

Ich empfehle der Finanzverwaltung, im Zusammenhang mit der Umstellung des Verfahrens von der Papier- auf die Elektronische Lohnsteuerkarte die erforderlichen technisch-organisatorischen Maßnahmen zu ergreifen, die einen unzulässigen Abruf der in der zentralen Datenbank gespeicherten Elektronischen Daten soweit wie möglich ausschließen. (Nr. 9.3).

Ich empfehle dem Gesetzgeber, die Abgabenordnung möglichst zeitnah um Regelungen zu einem voraussetzungslos gewährleisteten Auskunftsrecht des Steuerpflichtigen gegenüber der Finanzverwaltung zu erweitern (Nr. 9.4).

Ich empfehle dem Gesetzgeber, bei dem künftigen Verfahren zum Kirchensteuerabzug auf Kapitalerträge die besonderen Anforderungen zu beachten, die sich aus der Verwendung des sensiblen Merkmals der Religionszugehörigkeit ergeben. Kreditinstitute sollten Kenntnis von der Religionszugehörigkeit ihrer Kunden nur mit deren Einwilligung erhalten (Nr. 9.5).

Die neuen gesetzlichen Regelungen zum Scoring bedürfen weiterer Verbesserung (Nr. 10.5).

Trotz der neuen gesetzlichen Regelungen kommt die sog. SCHUFA-Klausel weiter zur Anwendung. Hier sollte der Gesetzgeber Klarheit schaffen (Nr. 10.6).

Ich empfehle der Bundesregierung, sich bei der Umsetzung der Interoperabilitätsrichtlinie zu europäischen Mautsystemen für die Beibehaltung des Verbots zweckändernder Nutzung von Mautdaten einzusetzen (Nr. 10.8).

Ich empfehle den am ELENA-Verfahren beteiligten Stellen, an den während der JobCard-Projekte und des Gesetzgebungsverfahrens zum ELENA-Verfahrensgesetz verabredeten Sicherheitsniveau keine Abstriche vorzunehmen (Nr. 11.1.3.1).

Ich empfehle dem Bundesministerium der Finanzen, dem Steuerpflichtigen bei der steuerlichen Berücksichtigung Beiträge zur privaten und gesetzlichen Kranken- und Pflegeversicherung (Vorsorgeaufwendungen) eine Alternative des Nachweises der Vorsorgeaufwendungen zur Verfügung zu stellen, beispielsweise durch Vorlage von entsprechenden Bescheinigungen beim Finanzamt (Nr. 11.1.6).

Ich empfehle den gesetzlichen Krankenkassen, meine „Empfehlungen zur Protokollierung in zentralen IT-Verfahren der Gesetzlichen Krankenversicherung“ zu beachten (Nr. 11.1.7).

Ich empfehle der DRV Bund, beim aktuellen und künftigen Einsatz medizinisch-technischer Geräte besonders darauf zu achten, dass beim beschriebenen Umgang mit diesen sensiblen personenbezogenen Daten die Persönlichkeitsrechte der Betroffenen gewahrt bleiben (Nr. 11.1.8).

Ich empfehle dem Gesetzgeber, mit Blick auf die Neugestaltung der Aufsichtszuständigkeiten meiner Behörde über die Jobcenter die zur Aufgabenerledigung notwendigen Planstellen einzurichten. Nur dann kann ich dauerhaft meinen gesetzlichen Auftrag erfüllen (Nr. 11.5.1).

Ich empfehle dem Gesetzgeber, bei der Schaffung des Beschäftigtendatenschutzgesetzes die Bestimmung über Datenabgleichverfahren so zu fassen, dass diese nur bei Vorliegen eines konkreten Anlasses zulässig sind. Die Regelungen zur Verwendung von Beschäftigtendaten zur Verhaltens- und Leistungskontrolle und zur offenen Videoüberwachung sollten enger gefasst werden. Der Umgang mit Daten bei der „gemischten“ dienstlichen und privaten Nutzung von Telekommunikationsdiensten sollte gesetzlich geregelt werden. Das Petitionsrecht des Beschäftigten darf nicht beschnitten werden (Nr. 12.1).

Ich empfehle der Bundesverwaltung, eine dauerhafte parallele Führung gleicher Teile der Personalakte – in Papierform und in eingescannter elektronischer Version – zu vermeiden und zeitlich auf ein Minimum zu reduzieren (Nr. 12.3).

Ich empfehle der Bundesregierung, sich beim weiteren Ausbau eines Raums der Freiheit, der Sicherheit und des Rechts auf europäischer Ebene für ein hohes Daten-

schutzniveau einzusetzen und die Kommission in ihrer Absicht zu unterstützen, das Datenschutzrecht auch im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zu modernisieren (Nr. 13.5).

Ich empfehle der Bundesregierung, in der Frage, in welchem Umfang Kunden- und Mitarbeiterdaten von deutschen Unternehmen mit den Antiterrorlisten der EU abzugleichen sind, weitere Schritte zu mehr Rechtssicherheit zu unternehmen (Nr. 13.7).

Ich empfehle dem Gesetzgeber, im Melderecht dem Schutz der Persönlichkeit einen hohen Stellenwert einzuräumen und hierfür erforderliche organisatorisch und informationstechnisch orientierte Vorgaben festzulegen (Nr. 15.12).

# 1 Modernisierung des Datenschutzrechts

## 1.1 Modernisierung des Datenschutzrechts – (k)eine endlose Geschichte?

*Nach punktuellen Verbesserungen des Datenschutzrechts muss die dringend erforderliche Grundrevision endlich in Angriff genommen werden.*

Die letzte größere Überarbeitung des BDSG liegt inzwischen zehn Jahre zurück. 1998 hatte sich die damalige rot-grüne Bundesregierung vorgenommen, das deutsche Datenschutzrecht grundlegend neu zu gestalten. Statt des großen Wurfs gab es aber im Jahr 2001 lediglich einen kleinen Schritt, der sich im wesentlichen auf die überfällige Anpassung des BDSG an die Europäische Datenschutzrichtlinie beschränkte, die 1995 in Kraft getreten war. Unmittelbar nach dieser Gesetzesnovelle sollte – so hatte es zumindest das Bundesinnenministerium angekündigt – die „Zweite Stufe" der Datenschutzreform in Angriff genommen werden. Zur Vorbereitung dieser grundlegenden Modernisierung hatte das BMI ein ausführliches Gutachten in Auftrag gegeben, das im Herbst 2001 fertig gestellt wurde (Roßnagel, Pfitzmann, Garstka, Modernisierung des Datenschutzrechts, 2001). Trotzdem ist es bis heute – trotz wechselnder politischer Mehrheiten – bei dieser Absichtsbekundung geblieben, obwohl die Dringlichkeit einer solchen Reform seitdem noch ständig gewachsen ist (vgl. zuletzt 22. TB Nr. 2.1).

Es ist allgemein anerkannt, dass eine Neukonzeption des Datenschutzrechts dringend erforderlich ist. Auch der Deutsche Bundestag hat entsprechende Schritte mehrfach angemahnt, so in seinen einstimmig getroffenen Entschließungen zu meinem 21. TB (unter Nr. 2, Anlage 4) und zum 22. TB (unter Nr. 1, 2, 3, Anlage 5).

Immerhin wurden im Berichtszeitraum punktuell einzelne Bereiche neu geregelt, bei denen aufgrund von Datenschutzskandalen und öffentlicher Diskussion der Handlungsbedarf besonders deutlich geworden war (vgl. Nr. 2.2 und 2.3). Die Grundstruktur des Datenschutzrechts harrt weiterhin der grundlegenden Überarbeitung.

Bisweilen drängt sich der Eindruck auf, dass der Reformstau im Datenschutzrecht inzwischen so groß ist, dass niemand mehr diese Mammutaufgabe in Angriff nehmen möchte. Ein derartiges Verharren auf dem rechtlichen Status Quo hätte angesichts zunehmender Herausforderungen verheerende Konsequenzen, bis hin zum sukzessiven Verlust der Privatsphäre der Bürgerinnen und Bürger.

Um Bewegung in die Modernisierung des Datenschutzes zu bringen, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe eingesetzt, die unter meiner Leitung konkrete Vorschläge für die Datenschutzreform erarbeitet hat. Die Datenschutzkonferenz hat im März 2010 das Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert" (vgl. Anlage 6) beschlossen und einer breiten Öffentlichkeit vorgestellt.

## 1.2 Eckpunkte der Datenschutzkonferenz – die Richtung ist vorgegeben

*Das Eckpunktepapier der Datenschutzkonferenz soll die Reformdiskussion in konkrete Bahnen lenken.*

Die Eckpunkte beschreiben die zentralen Herausforderungen für den Datenschutz, analysieren die jeweiligen Defizite der derzeitigen rechtlichen Rahmenbedingungen und ziehen daraus Schlussfolgerungen in Form konkreter Vorschläge für den Inhalt künftiger Regelungen.

Für die Gesamtkonzeption des Datenschutzrechts wird vorgeschlagen, zentrale allgemeingültige Schutzziele gesetzlich zu verankern, die einen verbindlichen Mindeststandard festlegen. Diese Schutzziele sollen die Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nicht-öffentliche Stellen bilden. Darauf basierend sollen zentrale Prinzipien, insb. die Erforderlichkeit, Zweckbindung und das Verbot der heimlichen Profilbildung, verankert und mit entsprechenden Sanktionsmöglichkeiten durchgesetzt werden.

Der Umgang mit personenbezogenen Daten sollte grundsätzlich offen und transparent sein, das Prinzip von Datenvermeidung und Datensparsamkeit soll verbindlich gelten und wirksamer durchgesetzt werden können. Darüber hinaus wird vorgeschlagen, für die Datenverarbeitung in verteilten Systemen (z. B. beim Cloud Computing) oder bei mehreren Beteiligten (z. B. bei zentralen Datenbanken, die von mehreren Stellen gemeinsam geführt werden) die datenschutzrechtlichen Verantwortlichkeiten so festzulegen, dass die Einhaltung des Datenschutzrechts und dessen Kontrolle besser handhabbar werden.

Für die Gewährleistung des technischen und organisatorischen Datenschutzes und der Datensicherheit sollten statt konkreter, auf eine bestimmte technische Umgebung fixierter Maßnahmen allgemeinverbindliche Schutzziele gesetzlich festgeschrieben werden. Damit wird ein technikneutraler und flexibler Ansatz geschaffen, der den grundrechtlichen Vorgaben des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auch bei sich verändernden technologischen oder organisatorischen Rahmenbedingungen Rechnung trägt (vgl. unten).

Datenschutz ist kein Selbstzweck; im Mittelpunkt steht der Einzelne, dessen Grundrechte durch die Verarbeitung seiner personenbezogenen Daten betroffen sind. Deshalb muss die Datenverarbeitung transparenter werden. Der Betroffene muss in der Lage sein, seine Rechte auf Auskunft, Berichtigung oder Löschung auf einfache Weise und auf elektronischem Wege wahrnehmen zu können. Entwickler und Verwender informationstechnischer Systeme sollten gesetzlich verpflichtet sein, datenschutzfreundliche Technik bereitzustellen und einzusetzen („Privacy by Design", vgl. Nr. 3.1). Den Betroffenen – die zunehmend selbst aktive Teilnehmer an IT-Verfahren sind und dabei persönliche Daten von sich und von Dritten verwenden – sollten IT-Produkte und Dienste mit den jeweils datenschutzfreundlichsten Einstellungen zur Verfügung gestellt werden („Privacy by Default").

Das Datenschutzrecht muss internetfähig werden. Dabei kommt der grundsätzlich unbeobachteten Nutzung elektronischer Dienste besondere Bedeutung zu. Es sind die Voraussetzungen zu schaffen, dass die Betroffenen auch im Netz ihre Rechte adäquat wahrnehmen können. Ebenso wie das Internet global ist, müssen auch datenschutzrechtliche Mindeststandards global gelten und durchgesetzt werden können.

Gesetzliche Regelungen für ein hohes und verbindliches Datenschutzniveau sind weiterhin wichtig. Zusätzlich müssen aber auch die Anreize gestärkt werden, dass die verantwortlichen Stellen Datenschutz als im eigenen Interesse liegendes Anliegen begreifen. Dies kann beispielsweise durch ein Datenschutzaudit geschehen, also die Zertifizierung der Datenschutzeigenschaften von Produkten und Diensten auf Basis unabhängiger Begutachtung. Ein durch gesetzliche Vorgaben in seiner Qualität gesichertes Datenschutzaudit könnte die Erfolgsaussichten datenschutzfreundlicher Angebote im Wettbewerb verbessern.

Die staatliche Datenschutzaufsicht und ihre Unabhängigkeit müssen gestärkt werden, um die Umsetzung der gesetzlichen Datenschutzanforderungen in der Praxis zu garantieren. So muss die personelle und finanzielle Ausstattung der Aufsichtsbehörden den gesteigerten Anforderungen entsprechen und sie benötigen wirksame Durchsetzungsbefugnisse. Die durch den Europäischen Gerichtshof in seinem Urteil vom 9. März 2010 festgelegten Anforderungen an die Unabhängigkeit der Datenschutzkontrolle (vgl. Nr. 2.1) müssen in Bund und Ländern zügig umgesetzt werden.

Die bei Verstößen gegen das Datenschutzrecht vorgesehenen Sanktionen haben sich zum Teil als nicht ausreichend erwiesen. Deshalb muss die Durchsetzung von Schadensersatzansprüchen sowie die Verfolgung von Ordnungswidrigkeiten erleichtert werden.

Schließlich muss das Datenschutzrecht insgesamt leichter lesbar und damit einfacher anwendbar werden. Durch die seit 1990 vorgenommenen zahlreichen Gesetzesänderungen haben einige Vorschriften des BDSG einen solchen Umfang angenommen, dass sie von den Rechtsanwendern – auch von solchen mit juristischer Vorbildung – bisweilen kaum noch verstanden werden. Zudem sind stellenweise sogar Widersprüche, Lücken und Überregulierungen entstanden, die fast zwangsläufig zu Unsicherheiten und Streit über die Auslegung der Bestimmungen führen.

Ich wünsche mir, dass unsere Eckpunkte die datenschutzpolitische Diskussion über die grundlegende Modernisierung auf eine neue Qualitätsstufe heben und im Ergebnis in entsprechende gesetzgeberische Aktivitäten münden. Ich sehe es positiv, dass der Deutsche Bundestag das Eckpunktepapier bereits positiv aufgenommen und die Bundesregierung aufgefordert hat, Möglichkeiten zu seiner Umsetzung zu prüfen (unter Nr. 6, Anlage 5). Selbstverständlich werde ich die Eckpunkte auch in die Diskussion über die Neuordnung des europäischen Rechtsrahmens (vgl. Nr. 13.2) einbringen.

Das vollständige Eckpunktepapier ist als Anlage 6 diesem Bericht beigefügt und ist in meinem Internetangebot veröffentlicht.

### 1.3 Datenschutz durch Technik und Organisation

*In den Reformvorschlägen der Datenschutzkonferenz kommt technischen und organisatorischen Komponenten eine wichtige Funktion zu.*

Das Bundesverfassungsgericht hat die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als neues Grundrecht aus Artikel 1 und 2 des Grundgesetzes hergeleitet (Entscheidung des Bundesverfassungsgerichts zum „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, 1 BvR 370/07 vom 27. Februar 2008). Damit werden diese beiden klassischen Schutzziele, die bereits in einigen Landesdatenschutzgesetzen ihren Niederschlag gefunden haben, in ihrer verfassungsrechtlichen Gültigkeit bestätigt. Bei den Überlegungen zu einer Weiterentwicklung der technisch-organisatorischen Regelungen in den Datenschutzgesetzen sollten deswegen folgende Bedingungen berücksichtigt werden:

1. Die Grundlage sollten elementare Schutzziele bilden, aus denen sich weitere (Schutz-)Ziele systematisch herleiten lassen. Die Schutzziele sollten einfach, verständlich und praxistauglich sein (vgl. Kasten zu Nr. 1.3).
2. Die Schutzziele korrespondieren mit den elementaren Schutzzielen der IT-Sicherheit (Verfügbarkeit, Unversehrtheit, Vertraulichkeit) und weisen mit diesen Überschneidungspunkte auf. Gleichzeitig sollte aber die spezielle Sichtweise des Datenschutzes zum Tragen kommen.
3. Die Schutzziele müssen nachhaltig sein, damit sie über längere Zeit Bestand haben.
4. Auf der Basis der Schutzziele sollten sich – anwendungsübergreifende und spezifische – Kataloge von Datenschutzmaßnahmen ableiten lassen, die – ähnlich wie der IT-Grundschutzkatalog des BSI – in flexible, praxistaugliche und durch Software unterstützte Verfahren umgesetzt werden können und als Kriterien-Kataloge eines Datenschutzaudits dienen könnten.
5. Die elementaren Schutzziele sollten weitgehend technologieunabhängig definiert werden, während die daraus abgeleiteten Maßnahmen den konkreten Anforderungen und Einsatzbedingungen der jeweiligen IT-Systeme Rechnung zu tragen haben. Somit gilt: Die Schutzziele bleiben, die Maßnahmen müssen sich dagegen weiterentwickeln.
6. IT-Systeme sind so zu gestalten, dass sie den grundlegenden rechtlichen Anforderungen des Datenschutzes entsprechen bzw. diese unterstützen (Datenvermeidung, Datensparsamkeit, Zweckbindung, Betroffenenrechte wie Berichtigung und Löschung). Dies greifen Konzepte wie Systemdatenschutz und Datenschutz

durch Technik (Privacy Enhancing Technology, PET) auf.

Beispielhaft:

- Löschbarkeit muss implementierbar sein
- technische Umsetzbarkeit von Betroffenenrechten (z. B. Auskunfts-, Berichtigungs- und Löschungsansprüche)
- Identitätsmanagement (Anonymisierung und Pseudonymisierung)
- revisionsfeste (d. h. auch durch die Systemadministration nicht zu verändernde) Protokollierung

7. Die technisch-organisatorischen Maßnahmen, die sich aus dem technischen Fortschritt ergeben sowie datenschutzfreundliche Techniken müssen angemessen abgebildet werden können.

Kasten zu Nr. 1.3

**Elementare Schutzziele des Datenschutzes**

| | |
|---|---|
| Verfügbarkeit: | Es ist zu gewährleisten, dass personenbezogene Daten und Verfahren zu ihrer Verarbeitung zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können. |
| Vertraulichkeit: | Es ist zu gewährleisten, dass nur befugt auf personenbezogene Verfahren und Daten zugegriffen werden kann. |
| Integrität: | Es ist zu gewährleisten, dass Daten aus personenbezogenen Verfahren unversehrt, zurechenbar und vollständig bleiben. |
| Transparenz: | Es ist zu gewährleisten, dass die Erhebung, Verarbeitung in personenbezogenen Verfahren und die Nutzung mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden können. |
| Zweckbindung: | Es ist zu gewährleisten, dass personenbezogene Verfahren so eingerichtet sind, dass deren Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können. |
| Intervenierbarkeit: | Es ist zu gewährleisten, dass personenbezogene Verfahren so gestaltet werden, dass sie dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen. |

Die technischen und organisatorischen Maßnahmen sollten im Sinne eines vorgelagerten Systemdatenschutzes nicht erst getroffen werden, wenn in einem Prozess feststeht, dass personenbezogene Daten verarbeitet werden sollen. Vielmehr ist die vielfach mögliche Personalisierung zunächst anonymer Daten oder die spätere Einbeziehung personenbezogener Daten zu berücksichtigen. Zu den in derartigen Fällen zu treffenden Vorkehrungen gehören auch solche, die eine unzulässige De-Anonymisierung oder Personalisierung von Daten verhindern.

### 1.4 Die öffentliche Diskussion hat begonnen

*Das Eckpunktepapier wurde einer breiten Öffentlichkeit vorgestellt.*

Um die Reformvorschläge der Fachöffentlichkeit vorzustellen und über die wichtigen Fragen mit Experten zu diskutieren, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 4. Oktober 2010 in Berlin ein Symposium zur Modernisierung des Datenschutzrechts veranstaltet (vgl. auch Nr. 14.1).

In zwei Fachvorträgen wurden grundsätzliche rechtliche und technologische Fragen thematisiert.

Die Staatssekretärin im Bundesministerium des Innern, Frau Cornelia Rogall-Grothe, erläuterte die Sichtweise der Bundesregierung. Sie begrüßte die Anregungen der Datenschutzbeauftragten, die mit dem Eckpunktepapier konkrete Verbesserungsvorschläge für das Datenschutzrecht vorgelegt hätten. Das Bundesinnenministerium sieht Handlungsbedarf vor allem bei der Verbesserung des Datenschutzes im Internet. Das BMI habe sich in der 17. Legislaturperiode verstärkt Fragen der Netzpolitik zugewandt, zu denen ganz entscheidend auch datenschutzrechtliche Themen gehören. Aus Sicht des BMI stehe dabei die Selbstregulierung im Vordergrund, etwa im Hinblick auf einen Kodex zum Umgang mit personenbezogenen Geodaten (vgl. Nr. 4.1.3).

Herr Prof. Dr. Friedemann Mattern von der Eidgenössischen Technischen Hochschule Zürich beleuchtete, welche technologischen Entwicklungen in naher Zukunft zu erwarten sind, welche Bedeutung diese für das Recht auf informationelle Selbstbestimmung haben und welche Möglichkeiten die Informationstechnik bietet, entstehende Risiken zu beherrschen. Besonderes Augenmerk richtete der Referent auf die Mobiltechnologie und die Möglichkeiten zur Verknüpfung von Daten über den Aufenthaltsort mit weiteren personenbezogenen Daten des Betroffenen. Damit würden reale und die virtuelle Welt immer stärker miteinander verknüpft und das persönliche Verhalten immer umfassender und genauer abgebildet.

In einer Podiumsdiskussion mit Vertretern aus Politik (Jan Philipp Albrecht, MdEP), Rechtswissenschaft (Prof. Dr. Michael Kloepfer), Informatik (Prof. Dr. Hannes Federrath), Wirtschaft (Prof. Dieter Kempf, BITKOM) und Datenschutzkontrolle (Dr. Alexander Dix) konnten dann einzelne Fragen vertieft diskutiert werden. Hierbei stand neben den bereits genannten Themen auch die europäische und internationale Dimension im Mittelpunkt. So sei es bedeutsam, dass die Eckpunkte der Datenschutzkonferenz in die Debatte um eine Neuordnung des europäischen Rechtsrahmens zum Datenschutz einflössen (vgl. Nr. 13.2). Einigkeit bestand darüber, auch international agierende Unternehmen mit Hauptsitz außerhalb Europas

stärker an das europäische Datenschutzrecht zu binden, soweit sie auf dem europäischen Markt tätig sind.

### 1.5 Wie geht es weiter mit IT und Datenschutz?

*Weiterhin gilt: Neue Informationstechnologien sind mit wachsenden Risiken für die Persönlichkeitsrechte verbunden. Sie durchdringen alle Lebensbereiche und bringen zusätzliche Kontrollpotentiale.*

Das Datenschutzrecht muss die technische Entwicklung berücksichtigen. Das ist leichter gesagt als getan, denn die Prognose technologischer Entwicklungen ist mit erheblichen Unsicherheiten verbunden. Die Formulierung allgemeiner Schutzziele (vgl. oben) und die Integration von technischen Neuerungen in einer abstrakten und technikneutralen Form in das Datenschutzrecht soll dem enormen Innovationstempo im Bereich der IT Rechnung tragen – eine anspruchsvolle Aufgabe!

Der Trend zu immer kleineren und leistungsfähigeren IT-Systemen hat sich auch in der Berichtsperiode ungebremst fortgesetzt. Auch die Vernetzung in der Informationstechnik schreitet unaufhaltsam voran.

Die Weiterentwicklung und Verknüpfung bisher getrennt voneinander betriebener IT-Systeme, neue Softwarekonzepte und Geschäftsmodelle eröffnen damit immer weiter gehende Kontrollpotentiale für staatliche Stellen und Unternehmen. Umso wichtiger wird es, diesen Risiken durch rechtliche Regelungen und technologische Lösungen Rechnung zu tragen, um die Persönlichkeitsrechte der Bürgerinnen und Bürger zu gewährleisten.

Grundlegende Forderungen zielen daher auf die Datensparsamkeit, die anonyme oder zumindest pseudonyme Nutzung von Diensten, den Einsatz datenschutzfreundlicher Identitätsmanagementsysteme, die Transparenz aller Verarbeitungsvorgänge und das Verbot der Bildung von Persönlichkeitsprofilen ohne Kenntnis und Einwilligung der Betroffenen. Schließlich ist es angesichts der zunehmenden Bedeutung und schnellen Entwicklung der Informations- und Kommunikationstechnologien dringlich, die IT-Kompetenz durch Aus- und Fortbildung in allen Bereichen unserer Gesellschaft zu erhöhen.

Die folgenden Beispiele sollen verdeutlichen, in welchem Maße informationstechnische Systeme zunehmend unseren privaten und beruflichen Alltag bestimmen und immer weitere Lebensbereiche umfassen:

- Soziale Netze
  Heute ist es selbst für Computerlaien ein Kinderspiel, persönliche Daten und Fotos im Internet zu veröffentlichen. Viele Menschen gehen mit diesen Möglichkeiten viel zu sorglos um und vertrauen private Daten – auch Daten Dritter – dem Internet an, ohne sich der Konsequenzen bewusst zu sein.
- Allgegenwärtige Datenverarbeitung (Ubiquitous Computing)
  Immer mehr Produkte sind mit Funkchips, sog. RFID-Tags (vgl. Nr. 5.9) ausgestattet, die im Umkreis von wenigen Zentimetern oder Metern („Nahfeld“) von stationären Kontrolleinheiten und von anderen „smarten Geräten“ erkannt werden können. Datenverarbeitung wird damit allgegenwärtig.
- Geolokalisierung
  Ungebrochen ist der Trend, ständig den Standort von mobilen Geräten (z. B. Smartphones, Laptops) über GSM- und WLAN-Netze zu bestimmen und diese Informationen – teilweise ohne Wissen des Nutzers – weiterzuleiten. Die so gewonnen Informationen können mit anderen Datenquellen (etwa elektronischen Telefon- und Adressverzeichnissen, Straßenansichten, Einträge in sozialen Netzwerken) zusammengeführt und zu Bewegungs-, Verhaltens- und Persönlichkeitsprofilen verdichtet werden.
- Biometrie
  Biometrische Erkennungsmethoden stehen zunehmend nicht nur staatlichen Stellen und Unternehmen zur Verfügung – sie können schon heute praktisch von jedermann eingesetzt werden. Ich halte es für beunruhigend, wenn anhand von Digitalfotos – die etwa mit Smartphones aufgenommenen wurden – beliebige Personen durch Abgleich mit im Internet oder in sozialen Netzen veröffentlichten Fotos identifiziert werden können.
- Cloud Computing
  Die Nutzung (standardisierter) Dienste über das Internet, wie beim Cloud Computing (vgl. Nr. 5.6) könnte die gesamte IT-Wirtschaft und -Nutzung umwälzen. Doch mit der IT aus der Steckdose (Software as a Service) dürfen die Verantwortung für die Datenverarbeitung und deren Kontrollierbarkeit nicht in der Wolke verschwinden.
- Konvergenz von Diensten und Netzen
  Die integrierte Nutzung von Internet, Sprachdiensten und Multimediainhalten multipliziert die spezifischen Risiken durch Wechselwirkungen zwischen diesen Diensten und Kumulationseffekte bei den Diensteanbietern.

### 1.6 Gibt es einen digitalen Radiergummi?

*Eigentlich sollte selbstverständlich sein, dass personenbezogene Daten auch wieder gelöscht werden können. Die Praxis sieht anders aus, insbesondere im Internet.*

Zu den Grundvoraussetzungen des Datenschutzes gehört es, personenbezogene Daten zu löschen, wenn sie für ihren Erhebungszweck nicht mehr benötigt werden oder nie hätten erhoben werden dürfen. Was nach der Rechtsprechung des Bundesverfassungsgerichts und den gesetzlichen Bestimmungen also eigentlich eine Selbstverständlichkeit ist, führt in der Praxis aber zu erheblichen Problemen (vgl. z. B. Nr. 5.4).

Weitgehend ungelöst ist die Frage der Datenlöschung im Internet, das seiner Natur nach auf weltweite Verbreitung und uneingeschränkte Nutzung der einmal eingestellten Informationen ausgerichtet ist. Die Probleme beginnen bei den Anbietern von Onlinediensten, die eine Funktion zum Löschen der einmal eingestellten Inhalte entweder

gar nicht vorsehen oder nur in unübersichtlichen Einstellungen, die schwer zu finden sind. Aber selbst wenn eine solche Funktion verfügbar ist und genutzt wird, bedeutet dies für die Nutzer nicht immer, dass ihre Daten tatsächlich entfernt werden. Oft bleiben sie gespeichert und können später analysiert werden.

Darüber hinaus stellen Onlinedienste oft technische Möglichkeiten bereit, um personenbezogene Daten weiteren Anbietern zur Verfügung zu stellen, die diese selbst noch einmal abspeichern und von einer späteren Löschung der Ursprungsdaten nichts erfahren.

Deswegen muss es das Ziel eines effektiven Datenschutzes im Internetzeitalter sein, dem Internet das Vergessen beizubringen oder einen „Radiergummi für das Internet“ zu entwickeln.

Bei näherem Hinsehen offenbart sich aber die Vorstellung, persönliche Informationen im Internet auf einfache Weise und nachhaltig löschen zu können, als kaum lösbares Problem. Der Radiergummi der realen Welt lässt sich in der digitalen nicht nachbilden, setzt er doch voraus, dass der Betroffene weiß, wo überall im Netz seine Daten veröffentlicht sind, und dass er tatsächlich „Herr seiner Daten“ ist.

Der Idee eines Verfallsdatums im Internet – unabhängig von den Vorgaben der jeweiligen Diensteanbieter – wurde kürzlich eine erste Form gegeben: Bei einem an der Universität Saarbrücken entwickelten System (x-pire) stellt der Betroffene seine persönlichen Daten in verschlüsselter Form ins Netz, beim Herunterladen durch andere Nutzer werden sie wieder entschlüsselt. Mit der Gültigkeitsdauer des dafür erforderlichen Schlüssels legt der Betroffene das Datum fest, bis zu dem seine Daten abrufbar sein sollen.

Die Lösung ruft einige kritische Fragen hervor – nach der Vertrauenswürdigkeit des Schlüsselverwalters oder wie man verhindern will, dass die heruntergeladenen Daten kopiert und an anderer Stelle wieder öffentlich gemacht werden. Ich halte sie aber dennoch für einen hilfreichen Beitrag zur Entwicklung neuer Ideen, um auch im Internet das Recht auf Löschung zu realisieren.

Weitere Ansätze sind erforderlich, um den Nutzerinnen und Nutzern eine möglichst weit gehende Kontrolle über die sie betreffenden Daten zu geben:

- Bereits bei der Erhebung müssen die Grundsätze der Datenvermeidung und -sparsamkeit gelten. So sollten die Dienste so gestaltet werden, dass nur die wirklich erforderlichen Daten erhoben und gespeichert werden. Die Inanspruchnahme der Dienste unter Verwendung von Pseudonymen sollte grundsätzlich möglich sein.
- Durch datenschutzfreundliche Voreinstellungen sollten die von den Nutzern eingestellten Inhalte zunächst nur einem von diesen selbst bestimmten begrenzten Kreis anderer Teilnehmer zugänglich gemacht werden. Die Veröffentlichung gegenüber einer allgemeinen, weltweiten Internetöffentlichkeit sollte nur erfolgen, soweit die Nutzer dies ausdrücklich wollen.
- Anbieter sollten verpflichtet werden, den Zugang der Betroffenen zu Löschfunktionen möglichst einfach und verständlich zu gestalten.
- Die Veröffentlichung personenbezogener Daten im Internet durch Dritte ohne Wissen des Betroffenen sollte gesetzlich geregelt und grundsätzlich von einer Einwilligung abhängig gemacht werden.
- Die technische Bereitstellung personenbezogener Daten durch Onlineanbieter an Dritte (etwa die Entwickler von Software, Anbieter von Spielen und sonstigen Diensten) sollte nur erfolgen, soweit dies vom Benutzer explizit genehmigt wurde, wobei er zuvor ausdrücklich darauf hinzuweisen wäre, welche Empfänger für welche Zwecke auf die Daten zugreifen, diese kopieren, speichern und auswerten können.

Technische und rechtliche Lösungen dieser Problematik sind dringend erforderlich, werden aber nur greifen können, wenn sie auch international akzeptiert und durchsetzbar sind. Deshalb sind die Bestrebungen zur europa- und weltweiten Verbesserung des Datenschutzes von herausragender Bedeutung (vgl. Nr. 13.2).

## 2 Datenschutzrechtlicher Rahmen

### 2.1 Lektion aus Luxemburg: Datenschutzaufsicht in Deutschland nicht unabhängig

*Wie der Europäische Gerichtshof (EuGH) mit Urteil vom 9. März 2010 (C-518/07) festgestellt hat, genügt die Datenschutzaufsicht im nicht-öffentlichen Bereich in Deutschland nicht den in der EG-Datenschutzrichtlinie 95/46 festgelegten Anforderungen an die völlige Unabhängigkeit. Die Feststellungen des Gerichts müssen jetzt zügig umgesetzt werden – nicht nur in den Ländern, sondern auch beim Bund.*

Die Europäische Kommission hatte das Verfahren eingeleitet (vgl. 21. TB Nr. 2.2), weil nach ihrer Ansicht die Organisation der Datenschutzaufsicht im nicht-öffentlichen Bereich in Deutschland gegen Artikel 28 Absatz 1 der EG-Datenschutzrichtlinie verstößt: Die Aufsichtsbehörden könnten ihre Aufgaben nicht in der geforderten „völligen Unabhängigkeit“ wahrnehmen. Dies betraf nicht nur die Länder, in denen die Datenschutzaufsicht bei Behörden der Innenverwaltung oder den Innenministerien selbst angesiedelt ist, sondern auch die, in denen die Datenschutzaufsicht im nicht-öffentlichen Bereich den Landesbeauftragten für den Datenschutz zugewiesen war.

Diese Auffassung wurde nun vom EuGH sehr weitgehend bestätigt. Nach seinem eindeutigen Urteil muss die Datenschutzaufsicht von jeder äußeren Einflussnahme frei sein. Völlige Unabhängigkeit bedeute nicht allein, dass eine Einflussnahme von den zu kontrollierenden Daten verarbeitenden Stellen auszuschließen sei (funktionelle Unabhängigkeit). Vielmehr sei der Begriff der völligen Unabhängigkeit in einem umfassenden Sinne zu verstehen. Es müsse gewährleistet sein, dass keinerlei politische und institutionelle Einflussnahme, etwa im Sinne einer Aufsicht

über die Datenschutzaufsichtsbehörde stattfinde. Schon der Anschein einer solchen möglichen Einflussnahme müsse ausgeschlossen werden.

Um das Urteil des EuGH umzusetzen, müssen in den meisten Bundesländern Änderungen bei der organisatorischen Stellung der Datenschutzaufsichtsbehörden vorgenommen werden. Denn in der Regel unterliegen die Aufsichtsbehörden einer Rechtsaufsicht oder sind unmittelbar Teil der Innenverwaltung und unterliegen sogar einer Fachaufsicht. Beides ist mit dem europäischen Recht unvereinbar. Eine Dienstaufsicht ist so weit zu beschränken, dass sie nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzbehörde führen kann. Hierfür bietet sich als Vorbild das Modell der richterlichen Unabhängigkeit der Mitglieder der Rechnungshöfe in Bund und Ländern an.

Infolge des Urteils sind daher in nahezu allen Ländern entsprechende Aktivitäten zu beobachten, um den vom EuGH definierten Anforderungen gerecht zu werden. Die weit überwiegende Zahl der Länder, in denen die Aufsicht über den nicht-öffentlichen Bereich noch von Behörden der Innenverwaltung ausgeübt wird, beabsichtigen, diese Aufgabe den Landesdatenschutzbeauftragten zu übertragen oder haben dies bereits getan.

Die 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18. März 2010 hat hierzu eine Entschließung verabschiedet, in der die zügige Umsetzung des Urteils angemahnt wird (vgl. Kasten zu Nr. 2.1).

Auch wenn sich das Urteil des EuGH formal lediglich auf die bei den Ländern angesiedelte Datenschutzaufsicht für den nicht-öffentlichen Bereich bezieht, wirkt es sich inhaltlich auch auf die Datenschutzkontrolle für den öffentlichen Bereich aus, denn die Anforderungen an die völlige Unabhängigkeit der Datenschutzkontrolle sind in der EG-Datenschutzrichtlinie nicht auf den nicht-öffentlichen Bereich beschränkt. Im öffentlichen Bereich kommt es sogar in noch viel stärkerem Maße darauf an, dass die Exekutive keinerlei Einfluss auf die Aufgabenwahrnehmung der Kontrollbehörde nehmen kann, denn die Exekutive wird ja ihrerseits durch die Datenschutzkontrollbehörde überwacht. Insofern gelten die vom EuGH aufgestellten Maßstäbe hier erst recht.

Deswegen muss auch meine Unabhängigkeit gestärkt werden, insbesondere im Hinblick auf meine Rechtsstellung. Der BfDI unterliegt in der Wahrnehmung seiner Aufgaben der Rechtsaufsicht der Bundesregierung. Auch wenn auf Grund der Rechtsaufsicht – anders als bei der Fachaufsicht – keine direkte Einflussnahme auf meine Entscheidungen ausgeübt werden kann, können doch grundlegende Interpretationsfragen von der Bundesregierung vorgegeben und damit Richtungsentscheidungen darüber, wie ich meine Aufgaben wahrnehme, festgelegt werden. Dies ist mit europäischem Recht nicht vereinbar. Auch wenn von der Rechtsaufsicht bisher noch kein Gebrauch gemacht wurde, widerspricht schon die Möglichkeit einer solchen Einflussnahme der durch die Richtlinie vorgegebenen völligen Unabhängigkeit. Zudem erweckt dies genau den Anschein der Einflussnahme, der nach dem Urteil des EuGH vermieden werden muss. Zudem ist die Dienstaufsicht des BMI über die Beschäftigten des BfDI und dessen Recht zur Stellenbesetzung ebenso zu hinterfragen wie die Bestellung des Leitenden Beamten durch das BMI.

Auch fehlt es mir im Hinblick auf die Datenschutzkontrolle bei Post- und Telekommunikationsunternehmen und öffentlich-rechtlichen Wettbewerbsunternehmen an den nach europäischem Recht notwendigen Durchsetzungsbefugnissen. So habe ich – anders als die Datenschutzbehörden der Länder – gegenüber den meiner Datenschutzkontrolle unterliegenden Unternehmen nicht die Möglichkeit, die unzulässige Verarbeitung personenbezogener Daten zu untersagen, betriebliche Datenschutzbeauftragte, die nicht den gesetzlichen Anforderungen genügen, abzuberufen oder Bußgelder zu verhängen. Stattdessen muss ich an die jeweiligen fachlichen Aufsichtsbehörden (etwa an die Bundesnetzagentur für die Bereiche Post und Telekommunikation) herantreten und diese zu überzeugen versuchen, selbst tätig zu werden. In der Vergangenheit hat es Fälle gegeben, bei denen ich anderer Auffassung war als diese gegenüber den Ministerien weisungsgebundenen Stellen.

Aber selbst diese Aufsichtsbehörden üben nicht dieselben Aufgaben aus wie die Aufsichtsbehörden für den Datenschutz gemäß § 38 BDSG und können – soweit ihnen nicht ausdrücklich weitergehende gesetzliche Befugnisse eingeräumt wurden – nur gegen Verstöße gegen spezialgesetzliche Regelungen (etwa gegen Datenschutzbestimmungen im TKG) vorgehen. Verstöße gegen sonstige Datenschutzbestimmungen – etwa gegen das BDSG – können sie hingegen nicht sanktionieren. Schließlich besitzen sie nicht die Befugnis, bei schwerwiegenden Verstößen die Datenverarbeitung zu untersagen oder betriebliche Datenschutzbeauftragte abzuberufen. Aus diesem Grund sollten dem BfDI für die genannten Bereiche die Befugnisse eingeräumt werden, die den Datenschutzaufsichtsbehörden der Länder zustehen. Dazu gehört auch die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem BDSG.

Das BMI sieht bislang allerdings keinen Handlungsbedarf, da die Rechtsstellung des BfDI nicht Gegenstand des Urteils gewesen sei.

Darüber hinaus muss auch die autonome Datenschutzaufsicht bei Religionsgemeinschaften und im Verwaltungsbereich der öffentlich-rechtlichen Rundfunkanstalten auf den Prüfstand, da auch hier eine völlige Unabhängigkeit im Sinne der europäischen Vorgaben nicht gegeben ist.

Unabhängig von seiner konkreten Umsetzung könnte das Urteil zum Anlass genommen werden, das zersplitterte System der Datenschutzaufsicht in Deutschland zu überprüfen. Gerade bei deutschland-, europa- und weltweit agierenden Unternehmen ist angesichts der Zuständigkeit einer Vielzahl von Aufsichtsbehörden trotz intensiver Abstimmung in Gremien und Arbeitsgruppen wie dem Düsseldorfer Kreis nicht immer eine effektive und schnelle Datenschutzaufsicht gewährleistet.

Kasten zu Nr. 2.1

**Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010**

**Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!**

Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Artikel 28 der Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt (Urteil vom 9. März 2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten.

Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

- Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.
- Es darf keine Fach- und Rechtsaufsicht geben.
- Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.
- Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.
- Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.
- Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.

## 2.2 Das lange Ringen um besseren Datenschutz

*Die dringenden Änderungen des Bundesdatenschutzgesetzes (BDSG) stießen auf unerwartet heftigen Widerstand und konnten zum Teil erst im letzten Moment und nur mit erheblichen Abstrichen beschlossen werden.*

Auch wenn die Diskussion über die Modernisierung des Datenschutzrechts im Berichtszeitraum kaum voran kam (vgl. Nr. 1), gab es in Einzelfragen durchaus Bewegung. Nachdem viele Jahre lang alle Forderungen nach dringend erforderlichen Änderungen im BDSG unerfüllt geblieben waren, sollte es plötzlich ganz schnell gehen. Ausgelöst durch eine Reihe von Datenschutzskandalen und das dadurch neu geweckte Interesse der Öffentlichkeit am Datenschutz hatten sich die parlamentarischen Gremien gleich mit mehreren Änderungsgesetzen zum BDSG zu befassen (vgl. 22. TB Nr. 2.2, 2.3 und 2.4).

Nach langer Vorbereitung ist als erstes der Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (Bundestagsdrucksache 16/10529) im August 2008 eingebracht worden, der verbesserte Datenschutzregelungen für die Tätigkeit von Auskunfteien und erstmals auch gesetzliche Vorgaben für Scoringverfahren enthielt. Obwohl die Bundesregierung in ihrer Gegenäußerung die umfangreichen Änderungsvorschläge des Bundesrates ganz überwiegend nicht aufgegriffen hatte, konnte der Entwurf in den Ausschussberatungen des Deutschen Bundestages noch in einigen Punkten deutlich verbessert werden (vgl. Beschlussempfehlung und Bericht des Innenausschusses, Bundestagsdrucksache 16/13219). In dieser Fassung wurde das Gesetz im Mai 2009 beschlossen (BGBl. I S. 2254) und ist am 1. April 2010 in Kraft getreten.

Wesentlich dramatischer verlief die Auseinandersetzung um das zweite Änderungsgesetz. Als Reaktion auf die durch Datenskandale einer breiten Öffentlichkeit deutlich gewordenen erheblichen Defizite beim Umgang mit personenbezogenen Daten von Millionen Bürgerinnen und Bürgern sollten endlich § 9a BDSG durch eine gesetzliche Regelung zum Datenschutzaudit ausgefüllt und der Handel mit insbesondere Adressdaten zu Werbezwecken eingeschränkt bzw. von der ausdrücklichen Einwilligung der Betroffenen abhängig gemacht werden (Gesetz zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, Bundestagsdrucksache 16/12011). Dieses Vorhaben der Bundesregierung stieß auf beispiellosen Widerstand aus Wirtschaftskreisen, die offensichtlich die personenbezogenen Daten der Bürgerinnen und Bürger als kostenlosen Rohstoff betrachteten, über den sie frei verfügen können müssten. Auch die Pläne zum Datenschutzaudit stießen auf erhebliche Kritik, u. a. weil sie als zu aufwändig und bürokratisch angesehen wur-

den und das Verhältnis der vorgesehenen Auditierung zur Kontrolltätigkeit der Aufsichtsbehörden der Länder nicht hinreichend geklärt sei. Wegen dieser Widerstände drohte das Gesetzesvorhaben insgesamt zu scheitern.

Erst in der letzten Sitzungswoche der ablaufenden Legislaturperiode des Deutschen Bundestags, also in allerletzter Minute, konnte ein Kompromiss gefunden und das Gesetz doch noch verabschiedet werden (BGBl. I S. 2814) und in wesentlichen Teilen zum 1. September 2009 in Kraft treten, allerdings nur nach erheblichen Veränderungen: So wurde die vorgesehene Regelung des Datenschutzaudits gestrichen. In der Beschlussempfehlung des Innenausschusses des Bundestags heißt es hierzu, vor einer gesetzlichen Regelung solle zunächst ein dreijähriges Pilotprojekt für eine Branche erfolgen. Dieser Aufforderung ist die Bundesregierung aber bislang nicht nachgekommen, wohl weil die von ihr geplante Stiftung Datenschutz möglicherweise auch ein Datenschutzaudit entwickeln soll. Auch der Adresshandel wurde nicht so geregelt, wie es die Bundesregierung ursprünglich beabsichtigt hatte. Insbesondere die Einwilligungslösung für die Verwendung von Daten zu Werbezwecken war gegen den geballten Widerstand der Wirtschaft offenbar nicht durchsetzbar, sodass sich hier für die Betroffenen leider nicht allzu viel zu ihren Gunsten geändert hat. Zur „Kompensation“ sind aber im Gesetzgebungsverfahren eine Reihe von zusätzlichen Änderungen in anderen Bereichen aufgenommen worden, die teilweise weitreichende positive Wirkungen entfalten, z. B. bei der Auftragsdatenverarbeitung oder die Informationspflicht bei Datenschutzpannen. In § 32 BDSG wurde zudem eine Grundregelung zum Beschäftigtendatenschutz aufgenommen (vgl. Nr. 12.1).

Schließlich wurde das BDSG auch noch durch Artikel 5 des Gesetzes zur Umsetzung der Verbraucherkreditlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht vom 29. Juli 2009 (BGBl. I S. 2355) geändert, mit dem EU-Richtlinien umgesetzt wurden.

### 2.3 Die Ergebnisse können sich – trotz allem – sehen lassen

*Der Datenschutz der Bürgerinnen und Bürger hat sich verbessert, wenn auch nur punktuell.*

Insgesamt lassen sich die recht zahlreichen Änderungen im BDSG positiv bewerten.

– Werbung und Adresshandel, Auftragsdatenverarbeitung, Informationspflicht bei Datenschutzpannen u. a. (vgl. Kasten a zu Nr. 2.3)

  Das Gesetz enthält wichtige Verbesserungen, die Bürgerinnen und Bürger besser gegen Datenmissbrauch schützen. Leider ist aber der im Herbst 2008 von der Bundesregierung zugesagte Wechsel hin zu einer Einwilligungslösung vor der Datenweitergabe für Werbezwecke nur inkonsequent eingeleitet worden: Die entsprechende Regelung enthält so viele Ausnahmen, dass sich hier in der Praxis keine großen Änderungen ergeben dürften. Die heftigen Auseinandersetzungen und die beispiellose Lobbykampagne haben gezeigt, dass beim Datenschutzbewusstsein in der Privatwirtschaft noch großer Nachholbedarf besteht. Die ersten Erfahrungen bei der Umsetzung der neuen Regel für Adresshandel und Werbung bestätigen zudem die Befürchtung, dass die gesetzlichen Bestimmungen nur schwer verständlich sind. Gerade interessierte Bürgerinnen und Bürger können durch einen Blick ins Gesetz nicht mehr erkennen, was Recht ist und was nicht.

  Die Unternehmen müssen die neuen Vorschriften nun mit Leben füllen. Wie ein roter Faden zieht sich durch alle Änderungen die Feststellung, dass viele Unternehmen den Bürgerinnen und Bürger im Umgang mit ihren personenbezogenen Daten keine effektiven Gestaltungsmöglichkeiten einräumen. Die Wirtschaft sollte das Bekenntnis des Gesetzgebers zum Vorrang der Einwilligung Ernst zu nehmen – trotz der Ausnahmemöglichkeiten. Unternehmen müssen sich intensiver Gedanken über die Umsetzung der informationellen Selbstbestimmung in ihrem Verantwortungsbereich machen und den Betroffenen die Kontrolle über ihre Daten zurückgeben.

– Auskunfteien und Scoring (vgl. Kasten b zu Nr. 2.3)

  Am 1. April 2010 traten verbesserte Datenschutzregeln für Auskunfteien in Kraft. Das Bundesdatenschutzgesetz regelt nun genauer, welche personenbezogenen Daten über eine Forderung an eine Auskunftei übermittelt werden dürfen. Zudem werden erstmals die Bedingungen für die Anwendung und Durchführung eines Scoringverfahrens gesetzlich definiert. Die Auskunftsansprüche der Betroffenen wurden gestärkt: insbesondere besteht zukünftig ein Anspruch auf kostenlose Auskunft, welche Scorewerte an Dritte übermittelt worden sind und wie der individuelle Scorewert zustande gekommen ist.

  Die ersten Erfahrungen mit den neuen Regelungen zeigen noch großen Nachholbedarf. Zwar ist der Anspruch auf jährliche kostenlose Auskunft auf großes Interesse der Betroffenen gestoßen. Der in der Theorie umfassende Auskunftsanspruch muss in der praktischen Anwendung aber noch beweisen, dass er tatsächlich zur Transparenz beiträgt, und nicht unnötige Formalismen und überlange Bearbeitungszeiträume diesen so wichtigen Anspruch ausbremsen.

– Verbraucherkreditrichtlinie

  Durch die am 11. Juni 2010 in Kraft getretene Umsetzung der Verbraucherkreditrichtlinie sichert § 29 Absatz 6 BDSG nunmehr die Gleichbehandlung von Darlehensgebern beim Zugang zu inländischen Auskunfteisystemen. Darlehensgeber aus anderen Mitgliedstaaten der Europäischen Union oder anderer Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum sind bei Auskunftsverlangen genauso zu behandeln wie inländische Darlehensgeber und dürfen unter denselben Bedingungen Auskünfte von Auskunfteien erhalten. Ich werde mit besonderer Sorgfalt beobachten, wie sich dies auf den Markt der Auskunfteisysteme auswirkt. Es gibt Auskunfteien, die auf einem Gegenseitigkeitsprinzip beruhen: Aus-

kunft erhält nur, wer seinerseits Informationen einmeldet. Es ist zu befürchten, dass in- und ausländische Auskunfteien versuchen werden, über diesen Weg ihr umfassendes Informationssystem auf die gesamte Europäische Union auszudehnen. Dies ist besonders deshalb problematisch, weil die im deutschen Recht vorgenommene Stärkung der Datenschutzrechte der Betroffenen in anderen EU-Staaten fehlt.

§ 29 Absatz 7 BDSG ist eine weitere Norm, die für mehr Transparenz sorgen soll. Beim Abschluss von Verbraucherdarlehensverträgen oder Verträgen über eine entgeltliche Finanzierungshilfe mit einem Verbraucher regelt das Gesetz nun ausdrücklich, dass der Verbraucher unverzüglich unterrichtet werden muss, wenn sein Vertragsangebot wegen einer (negativen) Auskunfteiabfrage abgelehnt wird.

Kasten a zu Nr. 2.3

**Die wichtigsten Änderungen im Überblick**

*Werbung und Adresshandel*

Seit dem 1. September 2009 dürfen personenbezogene Daten grundsätzlich nur noch mit Einwilligung des Betroffenen zu Zwecken der Werbung und des Adresshandels weitergegeben werden. Von diesem Grundsatz gibt es jedoch zahlreiche Ausnahmen, z. B.:

– Ohne Einwilligung kann Werbung versandt werden, wenn der Betroffene anhand der Werbung erkennen kann, welches Unternehmen seine Adressdaten hierfür weitergegeben hat.

  Dazu müssen Herkunft und Weitergabe der Adressdaten dokumentiert werden. Bereits aus der Werbung selbst muss sich ergeben, wer die Daten erstmalig weitergegeben hat. Diese Stelle muss dem Betroffenen dann auf Nachfrage mitteilen können, an wen sie seine Daten zu Werbezwecken in den letzten zwei Jahren weitergegeben hat. Hierfür gewährt der Gesetzgeber eine Übergangsfrist. Erst seit dem 1. April 2010 ist diese Pflicht verbindlich.

– Ohne Einwilligung dürfen Unternehmen auch ihre eigenen Kunden bewerben. Nutzen dürfen Sie hierfür sogenannte Listdaten, die sie beim Betroffenen selbst erhoben oder aus allgemein zugänglichen Quellen (etwa Telefonbüchern) entnommen haben. Jedoch dürfen nicht unterschiedslos alle Kundendaten für Werbezwecke herangezogen werden, sondern nur ein bestimmter Katalog listenmäßig oder sonst zusammengefasster Daten.

  Derartig zusammengefasst werden dürfen nur Angaben zu Name, Titel, akademischem Grad, Anschrift und Geburtsjahr, Berufs-, Branchen- oder Geschäftsbezeichnung sowie eine Angabe, die die Zugehörigkeit des Betroffenen zu einer bestimmten Personengruppe charakterisiert (z. B. Versandhauskunde).

Das Gesetz sieht für die von den Änderungen betroffenen Unternehmen eine Übergangsfrist von bis zu drei Jahren vor. Für Daten, die vor dem 1. September 2009 erhoben wurden, gilt daher die alte Rechtslage zunächst fort, d. h.:

– Daten, insbesondere zu Name, Anschrift, Geburtsjahr, Beruf sowie akademische Grade und Titel (die sogenannten Listdaten), können ohne Einwilligung des Betroffenen weiter wie bisher genutzt werden, und zwar
  – für Zwecke der Markt- oder Meinungsforschung bis zum 31. August 2010
  – für Zwecke der Werbung bis zum 31. August 2012.

*Koppelungsverbot*

Die Erbringung von Leistungen darf – jedenfalls bei marktbeherrschenden Unternehmen – nicht von der Einwilligung in die Datenweitergabe an Dritte abhängig gemacht werden. Damit wird die Freiwilligkeit von Einwilligungen gestärkt.

*Beschäftigtendatenschutz*

Mit § 32 BDSG wurde eine besondere Regelung zum Beschäftigtendatenschutz eingeführt. Kern der bisherigen Regelung ist eine strengere Zweckbindung der Verwendung von Beschäftigtendaten. § 32 BDSG soll aber lediglich Platzhalterfunktion haben und zukünftig durch umfassendere Regelungen ersetzt werden. Um diese Regelungen wird derzeit heftig gerungen (vgl. dazu Nr. 12.1).

*Auftragsdatenverarbeitung*

Auch die Regelungen zur Auftragsdatenverarbeitung werden verbessert. Dies betrifft etwa Callcenter, die in der Vergangenheit nicht immer als datenschutzrechtlich vorbildlich aufgefallen sind. Viele Skandale der letzten Zeit hatten ihre Ursache gerade in der unkontrollierten Datenweitergabe an Callcenter und andere Auftragnehmer. Der neue § 11

BDSG erschwert es dem Auftraggeber nunmehr, seine Verantwortung für die Rechtmäßigkeit der Datenverarbeitung auf den Auftragnehmer abzuwälzen und bürdet ihm eine strengere Kontrolle der Auftragnehmer auf (vgl. auch Nr. 2.4).

*Informationspflicht bei Datenschutzpannen*

Eine Melde- und Veröffentlichungspflicht bei schwerwiegenden Datenschutzverstößen soll es den Betroffenen und den Datenschutzbehörden zudem erleichtern, Folgeschäden zu vermeiden. Die Informationspflicht bei Datenschutzpannen ist gleichzeitig eine Chance zu besserem Datenschutzmanagement in den Unternehmen. Besser als eine transparente Informationspolitik nach einer Datenschutzpanne ist die Vermeidung solcher Pannen bereits im Vorfeld durch gutes Datenschutzmanagement.

*Betriebliche Datenschutzbeauftragte*

Neu ist ein besonderer Kündigungsschutz für betriebliche Datenschutzbeauftragte. Dadurch wird deren Unabhängigkeit gestärkt und ihr Wirken effizienter.

*Stärkung der Aufsichtsbehörden*

Schließlich werden auch die Befugnisse der Datenschutzbehörden wesentlich gestärkt. Sie können nun eine unzulässige Datenverarbeitung untersagen und höhere Bußgelder verhängen. Erstmals haben diese wirksame Handlungsmöglichkeiten erhalten und können strittige Auslegungsfragen (verwaltungs-)gerichtlich klären lassen.

K a s t e n b zu Nr. 2.3

**Die wichtigsten Änderungen im Überblick**

*Was darf eine Auskunftei sammeln?*

Der Gesetzgeber verbietet den Auskunfteien nicht, personenbezogene Daten zu verarbeiten und zu nutzen, um anhand dieser eine Aussage darüber treffen zu können, ob jemand seine Rechnung pünktlich bezahlen will und/oder kann.

Auskunfteien dürfen hierfür jedoch nicht jede Information heranziehen.

Bereits bisher war anerkannt, dass Unternehmen sogenannte Negativdaten verarbeiten dürfen. Dies sind Informationen darüber, dass Rechnungen und sonstige Zahlungsverpflichtungen nicht, nicht pünktlich oder nicht vollständig gezahlt worden sind. Nunmehr findet sich hierzu eine ausdrückliche gesetzliche Regelung in § 28a BDSG.

Danach dürfen personenbezogene Daten über eine Forderung an Auskunfteien übermittelt werden, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und es sich um eine der folgenden Forderungsarten handelt:

– Forderungen, die durch rechtskräftige Urteile festgestellt worden sind;
– Forderungen im Rahmen von Insolvenzverfahren;
– ausdrücklich anerkannte Forderungen;
– jede Art der Forderung, wenn Sie mindestens zweimal schriftlich gemahnt worden ist, auf die Einmeldung hingewiesen wurde und die Forderung nicht bestritten worden ist;
– jede Art von Forderung, die die verantwortliche Stelle zur fristlosen Kündigung berechtigt, wenn die verantwortliche Stelle den Betroffenen vorher über die Einmeldung bei einer Auskunftei informiert hat.

Zusätzlich dürfen Auskunfteien von Banken und anderen Kreditinstituten weitere positive Daten erhalten, nämlich Angaben über Girokontenverträge, laufende Kredite, beantragte Hypotheken oder andere Bankgeschäfte. Hinsichtlich eines Girokontos auf Guthabenbasis dürfen auf dieser Grundlage jedoch keine Angaben zu Bestehen, Ablauf, Dauer oder Beendigung des Girokontoverhältnisses an eine Auskunftei übermittelt werden.

Bisher musste hierzu eine so genannte „Einwilligungserklärung“ – freiwillig – unterschrieben werden (etwa die „SCHUFA-Klausel“). Ohne diese konnte der Vertrag bei Bank, Telefonunternehmen oder Versandhändler abgelehnt werden. Da die Freiwilligkeit bei solchen Erklärungen häufig jedoch nur auf dem Papier existierte, hat der Gesetzgeber nunmehr eine gesetzliche Regelung getroffen.

Doch nicht in allen Fällen ist eine Einwilligung nun überflüssig. Bereits bisher werden zur Bewertung seiner Zahlungsfähigkeit und Zahlungswilligkeit beispielsweise auch Informationen darüber gesammelt, wie viele Handyver-

träge ein Betroffener besitzt. Um diese Information erheben und verarbeiten zu dürfen, benötigen die Unternehmen auch weiterhin eine Einwilligung (vgl. hierzu Nr. 10.6).

*Was ändert sich beim Kreditscoring?*

Werden Scoringverfahren eingesetzt, um zu entscheiden, ob und zu welchen Bedingungen ein Vertrag abgeschlossen werden soll, dann müssen nunmehr nach § 28b BDSG bestimmte Bedingungen beachtet werden:

- Die Seriosität von Scorewerten muss wissenschaftlich nachgewiesen worden sein. Jede Stelle, die Scorewerte berechnet, muss der zuständigen Datenschutzaufsichtsbehörde darlegen können, dass die verwendeten Daten und die angewandte Methode tatsächlich geeignet ist, eine Aussage über das zukünftige Verhalten des Betroffenen zu treffen.
- Grundsätzlich darf eine Auskunftei alle Daten verwenden, die ihr über den Betroffenen bekannt sind. Nicht herangezogen werden dürfen aber etwa Daten, die nur gespeichert werden, um den Betroffnen bei einem Auskunftsverlangen sicher identifizieren zu können. Dies betrifft etwa die Speicherung von Voranschriften.
- Ein Scorewert darf nicht ausschließlich auf der Grundlage von Anschriftendaten ermittelt werden. Wenn Anschriftendaten für einen Scorewert herangezogen werden, spricht man von Geoscoring. Dies bedeutet, dass etwa die Bonität davon abhängig gemacht wird, in welcher Wohngegend jemand lebt. Eine solche Information zu verwenden, ist jedoch in höchstem Maße diskriminierend. Der Gesetzgeber wollte jedoch das Geoscoring nicht vollständig verbieten, sondern im Wesentlichen für den Betroffenen transparenter machen. Verboten ist es jedoch, einen Score ausschließlich auf die Wohngegend zu stützen. Also zur Berechnung des Scorewertes keine weiteren oder nur solche Angaben hinzuzuziehen, die keinen wesentlichen Einfluss auf die Entscheidung haben.

*Mehr Transparenz beim Scoring*

Der Scorewert muss verständlich, einzelfallbezogen und nachvollziehbar erklärt werden. Die Betroffenen haben ein Recht darauf zu erfahren, ob sie einen guten, mittleren oder schlechten Scorewert haben und es muss ihnen erklärt werden, weshalb dieser Wert so ausgefallen ist. Diese Auskunft soll die Betroffenen in die Lage versetzen, die Entscheidung zu verstehen und ggf. mit sachlichen Argumenten in Frage zu stellen. Die Auskunft soll so dabei helfen zu beurteilen, ob der Scorewert von der richtigen Datengrundlage ausgeht und ob im zu beurteilenden Fall Besonderheiten bei der Bewertung der Bonität ausreichend berücksichtigt worden sind. Es gibt jedoch keinen Anspruch darauf, die genaue Scoreformel, also das mathematische Berechnungsverfahren des Scorewertes erklärt zu bekommen.

Für die Auskunft verantwortlich ist grundsätzlich zunächst der jeweilige Vertragspartner, der den Scorewert angewendet hat. Dieser darf den Betroffenen aber an eine Auskunftei verweisen, wenn er selbst den Scorewert nicht errechnet, sondern von einer Auskunftei hinzugekauft hat (vgl. zum Scoring auch Nr. 10.5).

*Einmal im Jahr ist die Auskunft kostenlos*

Jeder hat das Recht, einmal im Jahr eine kostenlose Auskunft von einer Auskunftei zu erhalten. Für jede weitere Auskunft kann jedoch ein Entgelt verlangt werden, wenn die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken genutzt werden kann.

## 2.4 Strengere Anforderungen an die Auftragsdatenverarbeitung

*Immer häufiger werden Datenverarbeitungsprozesse Dritten übertragen. Die Anforderungen hierfür sind gestiegen.*

Im Zuge von Outsourcing, Straffung von Betriebsabläufen und Einsparmaßnahmen werden in wachsendem Umfang in Wirtschaft und Verwaltung Teilaufgaben und die damit verbundene Datenverarbeitung auf Dritte übertragen. Grundlage hierfür ist vielfach eine Auftragsdatenverarbeitung nach § 11 BDSG, obwohl nicht immer, wo dies behauptet wird, die rechtlichen Voraussetzungen hierfür tatsächlich erfüllt sind. Wegen ihrer großen Bedeutung in der Praxis beschäftigt mich diese Thematik seit vielen Jahren (vgl. 22. TB Nr. 2.5).

Bei den Datenschutzskandalen der letzten Jahre hat sich mehrfach ergeben, dass nicht die verantwortliche Stelle selbst die Rechtsverstöße begangen hat, sondern ein von ihr beauftragter Dritter oder ein wiederum von diesem beauftragter weiterer Subunternehmer. Im schlimmsten Fall weiß die verantwortliche Stelle gar nicht mehr, wo und von wem tatsächlich ihre personenbezogenen Daten verarbeitet werden, und verliert so faktisch die Kontrolle, obwohl sie datenschutzrechtlich weiterhin in der Verantwortung steht.

Deswegen lag es nahe, bei der Novelle des BDSG, mit der der Gesetzgeber auf die Skandale reagieren wollte (vgl. Nr. 2.2 und 2.3), auch die Vorschriften zur Auftragsdatenverarbeitung zu verschärfen und hierfür strengere Anforderungen im Gesetz zu verankern. In Abwandlung des ursprünglichen Regierungsentwurfs wurde § 11 BDSG

im Gesetzgebungsverfahren neu gefasst, in dem insbesondere der erforderliche Inhalt des schriftlich zu erteilenden Auftrags präzisiert und die Kontrollpflichten des Auftraggebers deutlich vergrößert worden sind (vgl. Kasten a zu Nr. 2.4). Diese neuen Bestimmungen sind ohne Übergangsregelung zum 1. September 2009 in Kraft getreten.

Da die Änderungen zunächst nur für § 11 BDSG galten, unterlagen die besonders schützenswerten Sozialdaten insoweit plötzlich einem geringeren Schutzniveau, weil das Sozialgesetzbuch eine eigenständige Vorschrift zur Auftragsdatenverarbeitung enthält, die zunächst unverändert blieb. Inzwischen ist aber die erforderliche Rechtsangleichung erfolgt (vgl. Nr. 11.1.2).

Die gesteigerten Anforderungen an eine Auftragsdatenverarbeitung haben in der Praxis eine Reihe von Fragen aufgeworfen. Strittig waren u. a. die Behandlung von Altverträgen, die Art und Weise, in der sich die verantwortliche Stelle von den technischen und organisatorischen Datenschutzmaßnahmen des Auftragnehmers zu überzeugen hat, der zeitliche Abstand der künftig regelmäßig durchzuführenden Kontrollen und die Anforderungen an die gesetzlich vorgeschriebene Dokumentation. Deswegen habe ich hierzu in einer „Handreichung“ meine Auffassung zusammengefasst und veröffentlicht (www.bfdi.bund.de; vgl. Kasten b zu Nr. 2.4).

Als Nebeneffekt hat die Änderung des § 11 BDSG zur Folge, dass in vielen Verwaltungen und in Unternehmen die internen Datenschutzbeauftragten erstmals bei Outsourcing-Maßnahmen beteiligt wurden. Dies ist zu begrüßen, auch wenn dadurch eigentlich nur Versäumnisse in der Vergangenheit bereinigt werden.

Von großer Bedeutung wird sein, die beschriebenen Änderungen für die Auftragsdatenverarbeitung auch auf europäischer Ebene nachzuvollziehen. Angesichts der immer stärkeren internationalen Verflechtungen in der Informationstechnik und der damit verbundenen Datenströme – mit teils grenzüberschreitender Auftragsdatenverarbeitung – ist es dringend erforderlich, dass hierbei jeweils die gleichen hohen Datenschutzstandards gewährleistet werden. Die begonnene grundlegende Überarbeitung des europäischen Rechtsrahmens für den Datenschutz (vgl. Nr. 13.2) bietet hierfür eine gute Gelegenheit.

Kasten a zu Nr. 2.4

Durch das Gesetz zur Änderung datenschutzrechtlicher Vorschriften, das am 1. September 2009 in Kraft getreten ist, ist auch **§ 11 BDSG** in mehreren Punkten geändert worden:

- in § 11 Absatz 2 Satz 2 BDSG ist der Inhalt des schriftlich zu erteilenden Auftrags präzisiert worden; ein Verstoß hiergegen ist jetzt nach § 43 Absatz 1 Nummer 2b bußgeldbewehrt;
- nach § 11 Absatz 2 Satz 4 BDSG muss sich der Auftraggeber vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen. Ein Verstoß hiergegen ist jetzt nach § 43 Absatz 1 Nummer 2b BDSG bußgeldbewehrt;
- nach Beginn der Auftragsdatenverarbeitung hat eine entsprechende Überprüfung in regelmäßigen Abständen erneut zu erfolgen (§ 11 Absatz 2 Satz 4 BDSG);
- das Ergebnis aller dieser Überprüfungen ist zu dokumentieren (§ 11 Absatz 2 Satz 5 BDSG).

Kasten b zu Nr. 2.4

Auszug aus der Handreichung des BfDI zu § 11:

„…

Zu den sich hieraus ergebenden Fragen vertritt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit folgende Auffassung:

1. Alle nach dem 1. September 2009 schriftlich erteilten Aufträge i. S. d. § 11 Absatz 2 Satz 2 BDSG müssen den neuen inhaltlichen Anforderungen entsprechen. Dies gilt auch für neue Aufträge, denen ein nach altem Recht geschlossener Rahmenvertrag zugrunde liegt, weil Auftraggeber und Auftragnehmer hier die Möglichkeit haben, sich hinsichtlich des neuen (Teil-/Unter-) Auftrages auf die neue Rechtslage einzustellen.

   Nach altem Recht erteilte Aufträge werden in vielen Fällen nicht oder nicht in allen Punkten den neuen inhaltlichen Anforderungen entsprechen. Das Gesetz sieht keine Übergangsregelung vor, eine Umstellung aller Altverträge wird aber notwendigerweise eine gewisse Zeit in Anspruch nehmen. Der BfDI geht davon aus, dass

   – Altverträge bei jeder inhaltlichen Änderung (auch nur in einzelnen Punkten) oder anstehenden Verlängerung insgesamt dem neuen Recht angepasst werden;

- Altverträge, die der bis zum 1. September 2009 geltenden Rechtslage schon nicht entsprochen haben sofort überarbeitet werden;
- alle übrigen Altverträge bis spätestens 31. Dezember 2010 umgestellt werden. Da sich die Rechtslage geändert hat, können sich die Auftragnehmer nicht einer solchen Neugestaltung der Verträge verwehren, zumal das Gesetz erklärtermaßen lediglich eine Präzisierung vorgenommen hat, die schriftlichen Aufträge also im Prinzip auch schon nach altem Recht entsprechende Regelungen hätten enthalten müssen.

2. Auch nach bisherigem Recht schon hatte sich der Auftraggeber von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. In welcher Form dies zu geschehen hat, bestimmt das Gesetz nicht, auch nicht nach der zum 1. September 2009 in Kraft getretenen Änderung, obwohl diese Regelung jetzt zumindest zum Teil bußgeldbewehrt ist.

   „Sich überzeugen“ ist aber auf jeden Fall mehr, als die Entgegennahme schriftlicher Erklärungen oder etwa eines Sicherheitskonzeptes, wenn dessen konkrete Umsetzung nicht in irgendeiner Form überprüft wird. Dies ergibt sich schon daraus, dass das „Sich überzeugen“ künftig regelmäßig erfolgen muss, was keinen Sinn ergeben würde, wenn die Abgabe schriftlicher Erklärungen des Auftragnehmers, er beachte alle vertraglichen Vorgaben, ausreichend wären. Im schriftlichen Bericht des BT-Innenausschusses (Bundestagsdrucksache 16/13657) heißt es hierzu, es werde davon abgesehen, vorzuschreiben, dass sich der Auftraggeber unmittelbar selbst vor Ort beim Auftragnehmer überzeugt. Als Möglichkeiten werden auch das Testat eines Sachverständigen oder eine schriftliche Auskunft des Auftragnehmers genannt. Diese muss sich nach Auffassung des BfDI dann aber auf konkrete Fragen des Auftraggebers beziehen und kann sich nicht auf allgemeine Erklärungen beschränken.

3. Nach § 11 Absatz 2 Satz 4 BDSG hat künftig die erste Überprüfung durch den Auftraggeber vor Beginn der Auftragsdatenverarbeitung stattzufinden. Dies kann bei derzeit bereits laufenden Auftragsdatenverarbeitungen naturgemäß nicht mehr beachtet werden. Wird ein solcher Auftrag allerdings erneuert oder umgestellt (s. o.), muss eine entsprechende Überprüfung durchgeführt werden, schon allein deswegen, weil in dem neuen, der Gesetzesänderung entsprechenden Auftrag Punkte enthalten sein werden, die bislang nicht vereinbart waren und deswegen auch nicht überprüft worden sind.

   Außerdem sollte in diesen Fällen so schnell wie möglich mit den ebenfalls vorgeschriebenen regelmäßigen Überprüfungen (vgl. Nr. 4) begonnen werden.

4. § 11 Absatz 2 Satz 4 BDSG sieht künftig neben der Anfangskontrolle vor Beginn der Auftragsdatenverarbeitung regelmäßige Überprüfungen vor. Dies gilt ab dem 1. September 2009 für alle Auftragsdatenverarbeitungen, unabhängig davon, ob der Auftrag vor oder nach dem 1. September 2009 erteilt worden ist. In all den Fällen, in denen eine Anfangskontrolle nicht hat stattfinden können, sollte jetzt unverzüglich mit den regelmäßigen Kontrollen begonnen werden. Zwar ist ein Verstoß hiergegen nicht bußgeldbewehrt, gleichwohl aber rechtswidrig und kann Gegenstand einer Beanstandung sein.

   Den zeitlichen Abstand der regelmäßigen Überprüfungen legt das Gesetz bewusst nicht fest, weil dies der in der Praxis vorkommenden Bandbreite an Auskunftsdatenverarbeitungen nicht gerecht werde. Es ist also im Einzelfall auf den Umfang der Auftragsdatenverarbeitung, das Gefährdungspotential für die Betroffenen, die Innovationsgeschwindigkeit und die Sensibilität der verarbeiteten personenbezogenen Daten abzustellen. Das kann Fristen von weniger als einem Jahr, aber auch längere Zeiträume zur Folge haben. Sind die Zeitabstände allerdings zu groß (etwa nur alle fünf Jahre), kann von einer regelmäßigen Überprüfung nicht mehr gesprochen werden.

   Das Ergebnis der (Anfangs- wie Regel-) Kontrolle ist zu dokumentieren (§ 11 Absatz 2 Satz 5 BDSG). Auch hier verzichtet der Gesetzgeber auf weitere Ausführungen zu Form und Inhalt der Dokumentierung unter Hinweis auf die Bandbreite von möglichen Auftragsdatenverarbeitungen. Der Begriff „dokumentieren“ beinhaltet aber bereits, dass dies in schriftlicher oder sonst nachvollziehbarer Form zu erfolgen hat. Nach Sinn und Zweck der Regelung muss aus der Dokumentation mindestens der Zeitpunkt der Überprüfung hervorgehen. Außerdem sollte daraus ersichtlich sein, was genau überprüft worden ist, in welcher Form dies geschehen ist und mit welchem Ergebnis.“

## 2.5 Stiftung Datenschutz nimmt Gestalt an

*Die geplante Stiftung Datenschutz kann den Datenschutz in Deutschland stärken, muss aber unabhängig sein und auf das bestehende System der Datenschutzaufsicht abgestimmt werden.*

In ihrem Koalitionsvertrag haben sich die Regierungsparteien für eine Stärkung des Datenschutzes ausgesprochen. Hierzu soll eine Stiftung Datenschutz beitragen, die Produkte und Dienstleistungen auf ihre Datenschutzfreundlichkeit hin prüfen, Bildung im Bereich des Datenschutzes stärken, den Selbstdatenschutz durch Aufklärung verbessern und ein Datenschutzaudit entwickeln soll. Nach Abschluss der konzeptionellen Vorarbeiten soll die Bundesstiftung im Laufe des Jahres 2011 errichtet werden.

Ich bin der Auffassung, dass die Stiftung Datenschutz zur Stärkung des Datenschutzes beitragen kann. Allerdings muss

sich das Stiftungskonzept in das System der Datenschutzaufsicht einfügen. Die Beurteilung, ob die datenschutzrechtlichen Anforderungen eingehalten sind, unterliegt weiterhin den Datenschutzaufsichtsbehörden. Insbesondere bei der Prüfung von Produkten und Dienstleistungen auf ihre Datenschutzfreundlichkeit hin und bei der Entwicklung und Vergabe von Datenschutzaudits durch die Stiftung muss daher sicher gestellt sein, dass sich die Stiftung nicht in Widerspruch zu der Kontrolltätigkeit der Datenschutzbehörden setzt. Gegenteilige Entscheidungen und Empfehlungen von Stiftung Datenschutz und Aufsichtsbehörden wären weder im Interesse der Daten verarbeitenden Stellen noch der Verbraucherinnen und Verbraucher.

Die 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits im November 2010 darauf hingewiesen, dass eine enge Kooperation zwischen der Stiftung Datenschutz und den Datenschutzaufsichtsbehörden unerlässlich ist (vgl. Kasten zu Nr. 2.5).

Kasten zu Nr. 2.5

**Entschließung der 80. Konferenz der der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010**

**Förderung des Datenschutzes durch Bundesstiftung**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt zur Kenntnis, dass die Bundesregierung mit Hilfe einer Stiftung den Datenschutz stärken will. Ungeachtet der noch zu klärenden verfassungsrechtlichen Vorfragen wird dieses Ziel von den Datenschutzbeauftragten nachdrücklich unterstützt. Dieses Vorhaben setzt voraus, dass

- die Stiftung ihre Aufgaben unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft wahrnimmt,
- die größtmögliche Transparenz der Tätigkeit garantiert ist und
- die Stiftung eng mit den Datenschutzbehörden des Bundes und der Länder kooperiert.

Die Stiftung kann nur solche Aufgaben übernehmen, die nicht ausschließlich den Datenschutzbehörden zugewiesen sind. Dies gilt insbesondere für die Kontrolle, ob gesetzliche Anforderungen eingehalten werden.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für angezeigt, möglichst frühzeitig in die Überlegungen zur Stellung und zu den Aufgaben der Stiftung einbezogen zu werden. Insoweit bieten sie der Bundesregierung ihre Unterstützung und Mitarbeit an.

Ich halte es darüber hinaus für angezeigt, dass die Datenschutzbehörden in den Gremien der Stiftung beteiligt werden, damit sie frühzeitig über anstehende Entscheidungen der Stiftung informiert werden und ihre Erfahrungen einbringen können.

Bei der Besetzung der Stiftungsorgane und der Finanzierung ist zudem die organisatorische und finanzielle Unabhängigkeit der Stiftung von den Daten verarbeitenden Stellen und der Wirtschaft zu garantieren. Nur so kann sie das für ihre Arbeit unverzichtbare Vertrauen der Bürgerinnen und Bürger in die Unabhängigkeit ihrer Arbeit gewinnen.

Die Stiftung Datenschutz könnte darüber hinaus auch als „Trust-Center“ für ein zentrales Widerspruchsregister gegen die Veröffentlichung personenbezogener Daten im Internet fungieren (vgl. Nr. 4.2).

## 2.6 Datenbrief – ein Vorschlag mit Tücken

*Die Idee, alle Betroffenen einmal jährlich unaufgefordert über die zu ihrer Person gespeicherten Daten zu informieren, ist ein anspruchsvolles Projekt, dessen Umsetzung allerdings schwierig sein dürfte.*

Anfang des Jahres 2010 sorgte ein Vorschlag des Chaos Computer Clubs für Diskussionen, alle Behörden, Unternehmen und Institutionen gesetzlich zu verpflichten, die Betroffenen unaufgefordert einmal jährlich über die zu ihrer Person erhobenen, gespeicherten oder übermittelten Daten zu unterrichten. Ein solcher „Datenbrief“ solle die Datensammelwut bremsen, Transparenz herstellen und die Möglichkeit der Betroffenen verbessern, ihre Rechte wahrzunehmen.

Diese Idee fand durchaus positive Resonanz in Politik und Gesellschaft, zeigte sie doch auch, wie wenig die im BDSG bereits enthaltenen Benachrichtigungspflichten wegen der vielfältigen Ausnahmen greifen. Der Bundesminister des Innern berief zur Prüfung des Vorschlags eine Projektgruppe aus Vertretern von Unternehmen, Verbänden und Behörden ein, in der auch ich vertreten war. Schnell zeigte sich, dass die umfassende Konzeption des Datenbriefes in vielen Bereichen nicht in die Praxis umgesetzt werden kann. So macht der Datenbrief wenig Sinn, wo auf Grund unmittelbarer vertraglicher Beziehungen die damit verbundenen Datenverarbeitungen auch für die betroffenen Bürgerinnen und Bürger offen liegen und sie ihre datenschutzrechtlichen Ansprüche ohne weiteres geltend machen können. Auch der Umfang eines Datenbriefs und die technische Abwicklung warfen viele Fragen auf, die letztendlich dazu geführt haben, dass der Vorschlag in dieser Form wohl keinen Eingang in das BDSG finden wird, etwa im Hinblick auf Fallkonstellationen, in denen zwar personenbezogene Daten gesammelt werden, die Identität der Betroffenen aber nur indirekt – durch Hinzuziehung weiterer Daten – festgestellt werden könnte.

Trotzdem hat die von dem Vorschlag ausgelöste Debatte erhebliche Defizite offengelegt, insbesondere im Hinblick auf die mangelnde Transparenz des Umgangs mit personenbezogenen Daten. Problematisch sind vor allem die – durchaus zahlreichen – Fälle, in denen Betroffene von Datenerhebungen, -speicherungen oder -übermittlungen überhaupt keine Kenntnis haben und ihr informationelles Selbstbestimmungsrecht deswegen auch nicht ausüben können. Dies gilt sowohl für die heimliche Erhebung von Daten im Internet (vgl. Nr. 4.1.2, 4.3) als auch für Bereiche, in denen Daten aus unterschiedlichen Quellen zusammengeführt werden, etwa zur – auch geschäftsmäßi-

gen – Weitergabe an Dritte oder zur Profilbildung. Hier halte ich mehr Transparenz für dringend geboten. Hier hat die Idee eines Datenbriefes durchaus weiterhin Bedeutung und sollte vom Gesetzgeber aufgegriffen werden, indem die gesetzlichen Benachrichtigungspflichten entsprechend verbessert werden.

### 2.7 Neuer Arbeitskreis Grundsatzfragen des Datenschutzes

*Der Arbeitskreis „Grundsatzfragen des Datenschutzes" der Datenschutzbeauftragten des Bundes und der Länder hat seine Arbeit aufgenommen.*

Alle Datenschutzbehörden sehen sich immer wieder mit grundsätzlichen Fragen konfrontiert, deren Beantwortung angesichts begrenzter Ressourcen große Schwierigkeiten bereitet. Die Bürgerinnen und Bürger, aber auch die für die Datenverarbeitung verantwortlichen Stellen erwarten zu Recht von den Datenschutzbeauftragten in Bund und Ländern, dass sie ihnen kompetente und abgestimmte Antworten auf diese grundlegenden Fragen geben. Da es bisher mangels entsprechender Strukturen zwischen den Datenschutzbehörden dazu wenig Austausch und Abstimmung gab, hat die 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18. März 2010 in Stuttgart einen neuen Arbeitskreis „Grundsatzfragen des Datenschutzes" eingesetzt.

Aufgabe des Arbeitskreises ist es, komplexe Themen intensiv zu beraten, in grundsätzlichen Fragen gemeinsame Positionen zu finden und diese Themenstellungen für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufzubereiten.

In den beiden ersten Sitzungen des Arbeitskreises hat sich der Arbeitskreis unter meinem Vorsitz u. a. mit der Modernisierung des Datenschutzrechts (vgl. Nr. 1), den Schlussfolgerungen aus dem Urteil des Europäischen Gerichtshofs vom 9. März 2010 zur Unabhängigkeit der Datenschutzkontrolle (vgl. Nr. 2.1), grundsätzlichen Fragen des Umgangs mit Geodaten (vgl. Nr. 4.1) oder den Datenschutzrechten juristischer Personen befasst.

## 3 Elektronische Identität

„Wer bin ich – und wenn ja wie viele?" lautet der Titel eines Sachbuchs von Richard D. Precht, das 2010 auf dem ersten Platz der Sachbuch-Bestseller-Liste stand. Ähnlich könnte man fragen, wenn es um unsere Identitäten im Internet, bei Behörden oder in Sozialen Netzwerken geht. Die Menge personenbezogener Daten bei staatlichen und privaten Stellen steigt ständig an. Durch die leichte Verknüpfbarkeit vieler Informationen können glaubwürdige, aussagekräftige Persönlichkeitsprofile des Einzelnen erstellt werden.

Beispiele für elektronische Identitäten sind die persönliche De-Mail-Adresse (vgl. Nr. 3.3), die Steuer-Identifikationsnummer (vgl. Nr. 9.2) oder Zugangskennungen zu einem Internet-Shop oder Sozialen Netzwerk.

Werden diese und ähnliche Daten ohne entsprechende Rechtsgrundlage verknüpft, ist das Recht auf informationelle Selbstbestimmung gefährdet. Deshalb sind Technologien erforderlich, die die Betroffenen selbst bestimmen lässt, welche elektronischen Identitäten wo verwendet werden. In den von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeiteten Eckpunkten „Ein modernes Datenschutzrecht für das 21. Jahrhundert" (siehe Nr. 1) wird auf die Notwendigkeit eines datenschutzfreundlichen Identitätsmanagements hingewiesen: „Das Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren."

Mit der Einführung des neuen elektronischen Personalausweises (vgl. Nr. 3.2) gewinnt das Thema Identitätsmanagement weiter an Bedeutung, denn Bürgerinnen und Bürger erhalten erstmals von staatlicher Seite eine elektronische Identität. Damit ist nicht nur die Authentisierung gegenüber elektronischen Portalen der Verwaltung und der Wirtschaft möglich, sondern auch die Nutzung von verschiedenen anwendungsbezogenen Pseudonymen.

Zum Schutz vor Identitätsdiebstahl und unzulässiger Profilbildung wird es immer wichtiger, für Bürgerinnen und Bürger die Möglichkeit zu einem selbstbestimmten Identitätsmanagement zuschaffen. Ein derartiges System muss für die Nutzer einfach bedienbar und transparent sein; aus technologischer Sicht sind standardisierte Schnittstellen und die Möglichkeit der unabhängigen Überprüfbarkeit zu fordern.

### 3.1 eID Funktion und Privacy-by-Design-Konzepte

*Angesichts des rapiden technologischen Wandels gilt es, die besonderen Erfordernisse des Datenschutzes bereits zu einem frühestmöglichen Zeitpunkt zu berücksichtigen.*

Neue technologische Systeme bergen oftmals versteckte Gefahren, die sich nur schwer beseitigen lassen, wenn die Grundkonzeption erst einmal feststeht. Umso sinnvoller ist es, etwaige Datenschutzprobleme schon in der Entwicklungsphase neuer Technologien festzustellen und zu prüfen. Dieser Ansatz wird als „Privacy by Design" (PbD) bezeichnet.

Der Gedanke, den technischen Datenschutz in IT-Systeme zu integrieren, ist nicht völlig neu. Im Erwägungsgrund 46 der Richtlinie 95/46 der Europäischen Union wird z. B. darauf verwiesen, dass sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen zu treffen sind, um insbesondere die Sicherheit zu gewährleisten.

PbD ist wertvoll für alle Arten von IT-Systemen, die für die Verarbeitung personenbezogener Daten vorgesehen sind oder eingesetzt werden. PbD sollte eine wesentliche Anforderung sein, die durch alle Produkte und Dienstleistungen zu erfüllen ist, welche Dritten und einzelnen Kunden zur Verfügung gestellt werden (z. B. WiFi-Router, soziale

Netzwerke oder Suchmaschinen). Viele Nutzer verfügen nur über eingeschränkte IT-Kenntnisse und sind daher nicht in der Lage, die einschlägigen Sicherheitsmaßnahmen selbst zu ergreifen, um ihre eigenen oder die personenbezogenen Daten Dritter zu schützen. Daher ist im Zusammenhang mit diesen IT-Verfahren stets ein Grundschutz im Sinne datenschutzrechtlicher Voreinstellungen erforderlich (Privacy by Default).

Darüber hinaus müssen Anbieter die Nutzer in die Lage versetzen, ihre personenbezogenen Daten besser zu schützen, indem sie beispielsweise geeignete Datenschutztools bereitstellen (Zugangskontrollen, Verschlüsselung, Vorkehrungen für die anonyme Nutzung).

Kasten zu Nr. 3.1

**Datenschutzziele**

Bei Entscheidungen über die Konzeption eines Verarbeitungssystems, seiner Beschaffung und seinem Betrieb sollten die nachstehend aufgeführten allgemeinen Zielsetzungen beachtet werden:

Datenvermeidung: Datenverarbeitungssysteme sollten so ausgelegt und ausgewählt werden, dass keine oder möglichst wenig personenbezogene Daten erhoben und verwendet werden.

Kontrollierbarkeit: Ein IT-System sollte den Betroffenen die wirksame Kontrolle über ihre personenbezogenen Daten geben. Die Zustimmungs- bzw. Widerspruchsmöglichkeit sollte durch technologische Mittel unterstützt werden.

Transparenz: Sowohl die Entwickler als auch die Betreiber von IT-Systemen haben sicherzustellen, dass die Betroffenen detailliert über die Funktionsweise der Systeme informiert werden.

Vertraulichkeit der Daten: IT-Systeme sind so zu konzipieren und zu sichern, dass nur entsprechend autorisierte Stellen Zugriff auf personenbezogene Daten haben.

Datenqualität: Die Datenverantwortlichen müssen die Datenqualität durch technische Mittel unterstützen. Einschlägige Daten sollten im Bedarfsfall für rechtmäßige Zwecke zugänglich sein.

Möglichkeit der Trennung: IT-Systeme, die für verschiedene Zwecke eingesetzt werden können oder in einer Mehrbenutzerumgebung betrieben werden (d. h. virtuell verbundene Systeme wie z. B. Data Warehouses, Cloud Computing) müssen sicherstellen, dass Daten und Prozesse, die für verschiedene Aufgaben oder Zwecke verwendet werden, sicher voneinander getrennt werden können.

PbD jedoch umfasst mehr als nur die Gewährleistung der Sicherheit. PbD beinhaltet auch den Gedanken, Systeme so zu konzipieren und konstruieren, dass der Umfang der verarbeiteten personenbezogenen Daten minimiert wird. Wesentliche Elemente der Datensparsamkeit sind die Trennung personenbezogener Identifizierungsmerkmale von den Inhaltsdaten, die Verwendung von Pseudonymen, die Anonymisierung oder möglichst baldige Löschung personenbezogener Daten. Gute Beispiele für PbD in Deutschland sind die elektronische Gesundheitskarte (eGK) (vgl. Nr. 3.5), der neue Personalausweis (nPA) (vgl. Nr. 3.3) oder das Verfahren elektronischer Entgeltnachweis (ELENA) (vgl. Nr. 3.9).

Der Grundsatz des Privacy by Design sollte für Technologieentwickler und -hersteller ebenso verbindlich sein wie für diejenigen, die für die Daten verantwortlich sind und über die Beschaffung und den Einsatz von IT-Systemen zu entscheiden haben. Sie sollten verpflichtet sein, dem technologischen Datenschutz bereits in der Planungsphase von IT-Verfahren und -Systemen Rechnung zu tragen. Die Anbieter von IT-Systemen und -Dienstleistungen sollten zeigen, dass sie alle erforderlichen Maßnahmen getroffen haben, um diesen Erfordernissen zu genügen.

Aus der zunehmenden Bedeutung, die dem Datenschutz bei der Entwicklung und beim Betrieb von IT-Systemen zukommt, ergeben sich auch zusätzliche Anforderungen an IT-Spezialisten. Aus diesem Grunde muss der Datenschutz wichtiger Bestandteil ihrer Ausbildung sein.

## 3.2 Neuer Personalausweis

*Der neue Personalausweis soll mehr können als der alte; aber ist er auch gut für den Datenschutz?*

Seit dem 1. November 2010 wird der neue elektronische Personalausweis (nPA) ausgegeben. Der neue Ausweis hat Scheckkartenformat und bietet über die „klassische“ Ausweisfunktion des bisherigen Sichtausweises hinaus den elektronischen Identitätsnachweis für die Bereiche E-Commerce und E-Government an. Daher besitzt der nPA neben zusätzlichen Sicherheitsmerkmalen einen Chip mit je einem abgeschotteten Bereich für die gespeicherten Biometriedaten, für die elektronische Identitätsfunktion (eID) und außerdem für eine qualifizierte elektronische Signatur. Der Chip enthält alle auf dem Ausweis aufgedruckten Daten außer der Größe, der Augenfarbe und der Unterschrift.

Nachdem der Gesetzentwurf zunächst eine obligatorische Speicherung der Fingerabdrücke vorgesehen hatte, hat sich – auch nach meiner Kritik – letztlich hierzu eine datenschutzfreundlichere Position durchgesetzt. Die Speicherung der Fingerabdrücke erfolgt danach im nPA nur auf ausdrücklichen Wunsch des Inhabers. Die Antragsteller sollten sich jedoch gut überlegen, ob sie diese sensiblen Daten im Ausweis speichern möchten. Schließlich sind Vorteile kaum zu erkennen, die eine Speicherung der Fingerabdrücke bringen könnte. Auch der damit verbundene Sicherheitsgewinn ist marginal.

Die biometrischen Daten sind nur für staatliche Stellen mit speziell zertifizierten Lesegeräten abrufbar, wie z. B. im Zusammenhang mit polizeilichen Identitätskontrollen. Ich begrüße, dass eine dauerhafte zentrale Speicherung von elektronisch vorliegenden Biometriedaten des nPA mit Ausnahme der Produktionsphase ebenso wenig vorgesehen ist, wie die Einrichtung eines zentralen Personalaus-

weisregisters. Ebenso positiv zu bewerten ist die Trennung der hoheitlichen Funktionen von der eID-Funktionalität für die Bereiche E-Government und E-Commerce.

Ziel der eID-Funktion ist es, Internetnutzern mehr Sicherheit und besseren Datenschutz zu bringen. Die Nutzung der eID-Funktion ist freiwillig. Der Personalausweis wird über 16-jährigen grundsätzlich mit aktivierter eID-Funktion ausgehändigt. Die Funktion kann in den Personalausweisbehörden auf Wunsch kostenfrei deaktiviert werden sowie bei Bedarf kostenpflichtig wieder reaktiviert werden. Für die Ausweis-PIN, die bei der elektronischen Identitätsfunktion eingesetzt wird, sollte weder das Geburtsdatum noch eine ähnlich unsichere Ziffernfolge genutzt werden. Wer die eID-Funktion nutzen möchte, sollte darauf achten, dass der Rechner, von dem die Funktion genutzt werden soll, frei von Schadsoftware ist. Dies bedeutet vor allem, dass der Rechner über einen aktuellen Virenscanner sowie eine Firewall verfügt und Sicherheitsupdates regelmäßig durchgeführt werden.

Zwar begrüße ich diese Empfehlungen. Kritisch sehe ich es aber, dass die Verantwortung für eine sichere Nutzung der eID-Funktion damit sehr weit in den Verantwortungsbereich der den nPA nutzenden Bürgerinnen und Bürger geschoben wird. Da die Chipkarten-Lesegeräte der Sicherheitsklasse 1 („Basislesegeräte“) über keine eigene Tastatur verfügen, muss bei diesen die PIN über die PC-Tastatur eingegeben werden. Ist der PC durch Spionagesoftware infiziert, könnten Hacker die PIN ausspähen. Um der Gefahr des Ausspähens der PIN mittels einer Schadsoftware bei der Eingabe über die Tastatur zu begegnen, empfehle ich die sichereren „Standard-“ bzw. „Komfortlesegeräte“ für den nPA einzusetzen, die über eine eigene integrierte Tastatur und ein Display verfügen. Leider hat die Bundesregierung aber im Rahmen ihres Konjunkturprogramms vor allem die Verbreitung der risikobehafteten Basislesegeräte gefördert. Ein Hinweis noch: Die Nutzung der qualifizierten elektronischen Signatur ist nur mit Komfortlesegeräten möglich.

Um die eID nutzen zu können, muss auf den PC eine spezielle Software, eine sog. Ausweis App installiert sein. Der vom BMI gesteckte enge Zeitrahmen für die Einführung des nPA mag dazu beigetragen haben, dass die erste Version der Ausweis App Sicherheitslücken aufwies. Insbesondere war nicht ausgeschlossen, dass durch eine gefälschte Version der App Schadprogramme (Trojaner, Viren) auf den PC des Nutzers geladen werden konnten. Diese Sicherheitslücke wurde inzwischen nach Angaben des BMI mit Auslieferung einer neuen Programmversion geschlossen.

Unternehmen und Behörden, die sich als Diensteanbieter im Internet mit Hilfe der eID-Funktion Gewissheit über die Identität des Kunden bzw. des Bürgers verschaffen wollen, müssen sich zunächst bei der Vergabestelle für Berechtigungszertifikate registrieren lassen. Von dort erhalten sie nach einer Überprüfung ein Berechtigungszertifikat. Die Vergabestelle prüft, welche Daten des Ausweises von den Diensteanbietern für den jeweiligen Zweck benötigt werden und von ihnen aus dem nPA ausgelesen werden dürfen. Mit dem Berechtigungszertifikat sind die Diensteanbieter für die Nutzerinnen und Nutzer eindeutig zu erkennen. Mit dem Zertifikat wird ein – je nach Geschäftszweck – unterschiedlich weiter Zugriff auf die Ausweisdaten eröffnet. So werden z. B. für eine Altersverifikation an einem Warenautomaten deutlich weniger Daten und insbesondere keine Adressdaten benötigt als beim Vertragsabschluss im Bereich des Versandhandels. Diesen am datenschutzrechtlichen Erforderlichkeitsgrundsatz ausgerichteten differenzierten Zugriff begrüße ich.

Kritisch sehe ich es aber, dass die Vergabe der Zertifikate allein auf Basis der Erklärungen und Informationen der Diensteanbieter beruht. Ich hätte es begrüßt, wenn auch eine Prüfung des tatsächlichen Datenschutzstandards vorgegeben worden wäre. Zudem stellen Verbraucherschützer die berechtigte Frage, wie ausgeschlossen werden kann, dass unseriöse Anbieter die Berechtigungszertifikate zur Irreführung von Verbrauchern nutzen, denn die Prüfung der Geschäftsmodelle selbst gehört nicht zu den Aufgaben des Bundesverwaltungsamts, das die Zertifikate vergibt.

Im Übrigen können die Bürgerinnen und Bürger den Zugriff auf die eID-Daten im Einzelfall auch weiter beschränken, als vom Berechtigungszertifikat vorgesehen. Diese individuelle Zugriffssteuerung durch die Betroffenen ist aus datenschutzrechtlicher Sicht ausdrücklich positiv zu bewerten.

Ich hoffe, dass die beim Bundesverwaltungsamt eingerichtete Vergabestelle für Berechtigungszertifikate die notwendige Unterstützung erfährt, um eine sachgerechte Prüfung sicherzustellen. Datenschutzrechtliche Leitlinien für die Vergabe von Berechtigungszertifikaten wurden in einer Arbeitsgruppe unter Beteiligung von Mitarbeitern der Landesbeauftragten für den Datenschutz, meines Hauses, des Bundesinnenministeriums und des Bundesverwaltungsamtes vorbereitet.

Der neue Ausweis ermöglicht auch, Online-Angebote pseudonym zu nutzen. Dabei wird nicht der Name, sondern ein Pseudonym übertragen. Nutzt ein Internetshop zum Beispiel einen Bezahlservice und vertreibt digitale Waren per Download, ist es prinzipiell möglich einzukaufen, ohne dass der Anbieter den Namen des Käufers und dessen Postadresse erfährt.

Als weitere Funktion kann die qualifizierte elektronische Signatur optional auf den Chip aufgebracht werden. Der Ausweisinhaber kann damit Dokumente, z. B. Verträge, rechtsverbindlich unterschreiben. Die qualifizierte elektronische Signatur muss bei einem Zertifizierungsdiensteanbieter beantragt und kann von diesem auf den Chip des Ausweises geladen werden. Das Aufspielen und die Nutzung sind kostenpflichtig.

Ich werde beobachten, wie sich der Datenschutz bei Nutzung der eID-Funktion entwickeln wird und ob sich mit dieser Funktion und der parallel angebotenen qualifizierten elektronischen Signatur das Identitätsmanagement im Internet verändern wird. Außerdem werde ich die Kontrolle der von öffentlichen Stellen betriebenen Lesegeräte zum Auslesen der biometrischen Daten auf mein Prüfpro-

gramm setzen, sobald diese in größerer Stückzahl in Betrieb genommen wurden.

Da die neuen Ausweise durch kommunale Stellen personalisiert und ausgegeben werden, ist die Gewährleistung des Datenschutzes und der IT-Sicherheit beim nPA ganz wesentlich von den dortigen organisatorischen und technischen Gegebenheiten abhängig. Die für die Datenschutzkontrolle in diesen Bereichen zuständigen Landesdatenschutzbeauftragten haben hier in der Anfangsphase erhebliche Mängel festgestellt. Es ist zu hoffen, dass es sich dabei nur um Startschwierigkeiten gehandelt hat.

### 3.3 De-Mail: Die sichere Kommunikation der Zukunft?

*Unter dem neuen Projektnamen De-Mail wurde das Vorhaben einer zuverlässigen und (rechts-)sicheren elektronischen Kommunikation auf den Weg gebracht. Trotz Berücksichtigung wichtiger datenschutzrechtlicher und -technischer Forderungen sind einige Fragen weiterhin offen.*

Über das De-Mail-Vorhaben (früher: Bürgerportale) habe ich in meinem letzten Tätigkeitsbericht (vgl. 22. TB Nr. 6.6) bereits berichtet. Mittlerweile hat die Bundesregierung den „Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften“ beschlossen (BR-Drucksache 645/10). Die parlamentarischen Beratungen dauerten bei Redaktionsschluss noch an.

Ziel des Projektes ist es, eine Infrastruktur für eine (rechts-)sichere elektronische Kommunikation aufzubauen. Dazu gehört neben einem Postfach- und Versanddienst auch eine geschützte Dokumentenablage. Die Übertragung von Nachrichten erfolgt generell über einen verschlüsselten Kanal (zum Ablauf vgl. Kasten zu Nr. 3.3). Nachrichten werden unterwegs auf Schadsoftware geprüft und es werden Versandbestätigungen sowie – bei Bedarf – Empfangsbestätigungen verschickt. Behörden können sich zum Nachweis der Zustellung Abholbestätigungen ausstellen lassen.

Im Laufe des Gesetzgebungsverfahrens konnten einige wichtige datenschutzrechtliche Verbesserungen durchgesetzt werden. So wird neben der obligatorischen Transportverschlüsselung durch eine optionale Ende-zu-Ende-Verschlüsselung vom Sender bis zum Empfänger die Grundlage geschaffen, De-Mails gegen jegliches Mitlesen abzusichern. Dem Anspruch von Dritten, Auskunft über die Kommunikation und die Daten von De-Mail-Nutzern zu erhalten, wurden klare Grenzen gesetzt.

Es ist vorgesehen, dass ein De-Mail-Dienst nur durch E-Mail-Provider angeboten werden darf, die vom Bundesamt für Sicherheit in der Informationstechnik akkreditiert wurden. Eine der Voraussetzungen für die Erteilung der Akkreditierung ist eine Zertifizierung potentieller Diensteanbieter hinsichtlich der Erfüllung datenschutzrechtlicher Kriterien. Der Regierungsentwurf des De-Mail-Gesetzes sieht vor, dass der Diensteanbieter ein Gutachten eines Datenschutzsachverständigen einholt, das mir zur Überprüfung vorgelegt wird. Bei einer positiven Prüfung des Gutachtens erteile ich ein Datenschutzzertifikat, das der Diensteanbieter dem BSI als zuständiger Behörde vorlegen muss.

Die Datenschutzprüfung basiert auf einem Kriterienkatalog, der in meiner Verantwortung liegt. Eine vorläufige Fassung des Kriterienkataloges wurde von mir am 19. Januar 2011 veröffentlicht und ist auf meiner Internetseite unter http://www.datenschutz.bund.de abrufbar. Die verbindliche Version wird mit Inkrafttreten des De-Mail-Gesetzes im elektronischen Bundesanzeiger veröffentlicht.

Einige datenschutzrechtliche Bedenken wurden im laufenden Gesetzgebungsverfahren zumindest bisher nicht berücksichtigt. Hier sind weitere Verbesserungen erforderlich:

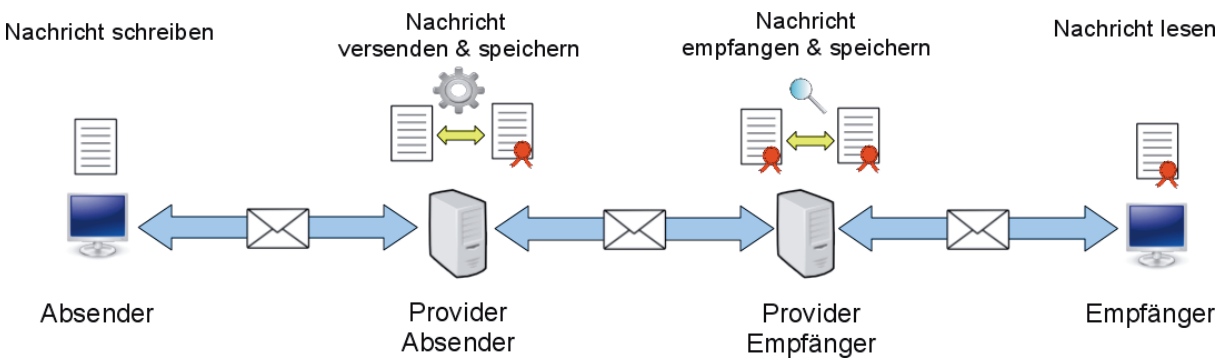
– Zukünftig sollen De-Mail-Nutzer ihren Schriftverkehr mit den Behörden verschlüsselt auf den Servern ihrer De-Mail-Diensteanbieter ablegen können. Um die sichere Ablage von sensiblen Dokumenten zu unterstützen, müssen De-Mail-Anbieter einen Dokumentensafe („De-Safe“) bereitstellen. Darin können die Nutzer Unterlagen gegen Manipulation und Verlust geschützt ablegen. Zur Sicherstellung der Vertraulichkeit und Integrität des Verfahrens sollte diese Sicherung durch eine ausschließlich vom Nutzer zu steuernde Verschlüsselung erfolgen.

– Meiner Forderung nach einer Verkürzung der im Rahmen der Dokumentationspflichten der Diensteanbieter vorgesehenen Speicherungsfristen von 30 Jahren für die Protokollierung der Kontoeröffnung, jeder Datenänderung sowie Sperrung oder Kündigung des De-Mail-Kontos wurde leider nur zum Teil nachgekommen. Speicherfristen sollten sich am Grundsatz der Datensparsamkeit orientieren und wesentlich kürzer sein. Gegebenenfalls wären auch differenzierte Fristen für unterschiedliche Datenarten denkbar.

Offen bleibt die Frage, ob De-Mail oder ähnliche Dienste wie der E-Postbrief (vgl. Nr. 6.8) für den Versand von besonders schützenswerten Daten geeignet sind. Bei sensiblen Daten wie beispielsweise Gesundheitsdaten ist es aus meiner Sicht zwingend erforderlich, die bestehenden Sicherheitsmaßnahmen um einen zusätzlichen Schutz wie eine Ende-zu-Ende-Verschlüsselung zu ergänzen.

Grundsätzlich befürworte ich das Ziel einer sichereren und verlässlicheren elektronischen Kommunikation. Im Zeitalter des elektronischen Versands von Rechnungen, Kontoauszügen oder Zugangsdaten für Internetportale wird es zwingend erforderlich, zusätzliche Sicherheitsmaßnahmen für die elektronische Kommunikation bereitzustellen. Entscheidend wird es jedoch sein, welche Akzeptanz De-Mail bei den Bürgerinnen und Bürgern finden wird. Und diese hängt nicht zuletzt von der Sicherheit, dem Datenschutz und der Transparenz des Verfahrens ab.

**Ablauf der Kommunikation über De-Mail**




## 3.4 Elektronische Gesundheitskarte

*Die elektronische Gesundheitskarte stand lange auf der Kippe, aber nach einem durch die Politik ausgesprochenem Moratorium sollte in diesem Jahr der Start gelingen, allerdings in einer deutlich abgespeckten Version. Keine Abstriche darf es aber beim Datenschutz geben.*

Die jetzige Krankenversichertenkarte wird bis spätestens zum 1. Januar 2006 zu einer elektronischen Gesundheitskarte erweitert. So steht es zumindest im Gesetz, aber die Realität sieht anders aus, wie ich bereits in meinen letzten Tätigkeitsberichten ausführlich berichtet habe (zuletzt 22. TB Nr. 6.1). Nachdem in den Testregionen die vorgesehenen Tests immer schleppender und ohne verwertbare Ergebnisse verliefen, vereinbarte die neue Bundesregierung in ihrem Koalitionsvertrag vom 26. Oktober 2009 vor einer weitergehenden Umsetzung eine Bestandsaufnahme vorzunehmen, bei der Geschäftsmodell und Organisationsstrukturen der gematik und ihr Zusammenwirken mit der Selbstverwaltung und dem Bundesministerium für Gesundheit, sowie die bisherigen Erfahrungen in den Testregionen überprüft und bewertet werden sollten.

Diese Bestandsaufnahme wurde im April 2010 abgeschlossen. Die Gesellschafterversammlung der gematik entschied sich für eine neue Verteilung der Aufgaben und Verantwortlichkeiten: Demnach übernehmen die Leistungserbringer die alleinige Verantwortung für die medizinischen Anwendungen und die Kostenträger die alleinige Verantwortung für die administrativen Anwendungen. Darüber hinaus verständigte man sich darauf, zunächst lediglich drei Anwendungen einzuführen, mit denen direkt beim Start ein Nutzen für alle Beteiligten erreicht werden soll:

- Ein online gestütztes Versichertenstammdatenmanagement (durch den GKV-Spitzenverband),
- die Einführung eines Notfalldatensatzes auf der elektronischen Gesundheitskarte (durch die Bundesärztekammer) und
- die adressierte Kommunikation der Leistungserbringer (durch die Kassenärztliche Bundesvereinigung).

Ferner wurde vereinbart, dass für die übergreifende Aufgabe der Basis-Telematikinfrastruktur der GKV-Spitzenverband gemeinsam mit der Kassenärztlichen Bundesvereinigung zuständig ist und es bei strittigen Entscheidungen ein Schlichtungsverfahren geben soll.

Durch das Gesetz zur Änderung krankenversicherungsrechtlicher und anderer Vorschriften vom 24. Juli 2010 (BGBl. I S. 983 ff.) wurde in § 291 Absatz 2b SGB V für den bis dahin nicht geregelten Versichertenstammdatendienst eine gesetzliche Grundlage geschaffen. Danach müssen die Leistungserbringer zwar einen online durchzuführenden Abgleich bei den Krankenkassen vornehmen, dies setzt aber nicht voraus, dass auch ihre Praxisverwaltungssysteme online genutzt werden müssen. Damit wird den Anforderungen nach Datensicherheit, Missbrauchsbekämpfung sowie der Forderung der Kostenträger nach einer Gültigkeitsprüfung und schnellen Aktualisierung der elektronischen Gesundheitskarte beim Leistungserbringer ebenso Rechnung getragen wie der Freiwilligkeit der Leistungserbringer zur direkten Anbindung ihrer Primärsysteme.

Zum Ende des Berichtszeitraums habe ich festgestellt, dass die verantwortlichen Gesellschafter intensiv an der Umsetzung der neuen Projektstrukturen arbeiten; erste Spezifikationen und Lastenhefte für die einzelnen Anwendungen liegen bereits vor, so dass mit einer abschließenden Beschlussfassung durch die gematik im Frühjahr nächsten Jahres zu rechnen ist. In der Region Nordrhein soll der Basis-Rollout der Lesegeräte in den einzelnen Arztpraxen und Krankenhäusern fortgesetzt werden, um danach mit einer Ausgabe in ganz Deutschland fortzufahren.

Die schleppende Einführung der elektronischen Gesundheitskarte wirft auch verschiedene datenschutzrechtliche Fragen auf. Ein Beispiel: Die bisher ausgegebenen elektronischen Gesundheitskarten der Generation 1 sind mit einer Verschlüsselungstechnologie ausgestattet, deren Kryptoalgorithmen nach der maßgeblichen BSI-Richtlinie TR-03116 bis zum Jahr 2015 zulässig sind. Bislang sind die für die Ausgabe der elektronischen Gesundheitskarten

verantwortlichen Krankenkassen – in Übereinstimmung mit der Industrie – davon ausgegangen, dass aus betriebswirtschaftlichen Überlegungen eine Karte mindestens fünf Jahre im Gebrauch sein sollte. Demzufolge stellt sich die Frage, ob der weitere Rollout der Karten der Generation 1 überhaupt noch sinnvoll ist oder ob man schon auf die Karten der Generation 2 umstellen muss. Das Problem wird sich vermutlich dadurch lösen, dass das BSI eine Laufzeitverlängerung der algorithmischen Schlüssel bis zum Jahr 2017 vornimmt.

Unzufrieden bin ich damit, dass das von mir seit Jahren kritisierte Problem der nicht geschützten Versichertendaten auf der jetzigen Krankenversichertenkarte weiterhin ungelöst bleibt (vgl. 22. TB Nr. 6.1). Hier habe ich der Zusage des BMG nach Abhilfe Glauben geschenkt, musste aber feststellen, dass die Umsetzung durch den bis heute nicht flächendeckend vorgenommenen Basis-Rollout nicht eingehalten worden ist (vgl. auch Nr. 15.6). Lange kann und darf dieser Zustand nicht mehr andauern, sonst werde ich dieses Verfahren beanstanden.

### 3.5 Biometrie bei der Grenzkontrolle

*Bei Personenüberprüfungen und Grenzkontrollen sollen biometrische Verfahren zur Verifizierung von Personen anhand der vorgelegten Ausweise verwendet werden.*

Seit 2004 wird Biometrie bei der Grenzkontrolle am Flughafen in Frankfurt am Main eingesetzt. Darüber habe ich bereits mehrfach berichtet (vgl. 20. TB Nr. 5.3.5; 21. TB Nr. 4.5.2). Mangels elektronischer Reisedokumente war das Verfahren „Automatisierte und biometriegestützte Grenzkontrolle (ABG)“ darauf angewiesen, dass biometrische Daten auf freiwilliger Basis lokal durch die Bundespolizei gespeichert wurden.

Mit der Einführung des neuen elektronischen Reisepasses ist es nun möglich, ohne vorherige Anmeldung und externe Datenspeicherung den Ausweis unmittelbar zur Verifikation einzusetzen. 2009 erfolgten ebenfalls am Frankfurter Flughafen erste Tests für einen automatisierten Kontrollprozess mit einem Gesichtserkennungsverfahren im Projekt „EasyPASS“ (vgl. 22. TB Nr. 6.4). Als technische und organisatorische Rahmenbedingungen wurde hierfür eine Kontrollspur mit guter Gesichtsausleuchtung eingerichtet. Um die Effizienz der Erkennung auf einem hohen Niveau zu halten, wurden dabei Erkenntnisse aus vorangegangenen Biometrieprojekten des Bundes genutzt. Es wird hierbei eine höhere Erkennungsgenauigkeit und eine beschleunigte Verifikation der Person mit den Daten des vorgelegten Reisepasses bzw. des neuen Personalausweises (vgl. Nr. 3.2) erwartet. Dies soll das Kontrollpersonal entlasten und den Passagierfluss beschleunigen. Zugleich sollen beim Kontrollprozess datenschutzfreundliche Rahmenbedingungen für die Bürger geschaffen werden.

Die Teilnahme an EasyPASS ist ohne vorherige Registrierung möglich und erfolgt derzeit noch auf freiwilliger Basis. Jeder volljährige Bürger der Europäischen Union, des Europäischen Wirtschaftsraums und der Schweiz, der über einen E-Pass verfügt, kann das Verfahren EasyPASS nutzen.

Der Reisende legt zunächst seinen Ausweis auf einen Dokumentenleser. Dabei werden seine Daten erfasst und es erfolgt eine Prüfung, ob der Reisende aufgrund der Ausweisdaten am automatisierten Kontrollprozess teilnehmen kann. Als kritisch betrachte ich in diesem Zusammenhang, dass zu jedem Reisenden eine Abfrage im nationalen bzw. im Schengen-Fahndungsbestand durchgeführt wird. Dies entspricht nicht dem Schengener Durchführungsübereinkommen bzw. dem Schengener Grenzkodex. Danach dürfen Personen, die das Gemeinschaftsrecht auf freien Personenverkehr genießen, nicht systematisch mit den Beständen nationaler und europäischer Datenbanken abgeglichen werden. Ich habe das BMI um Überprüfung des Verfahrens gebeten.

In der Kontrollschleuse wird das Gesichtsbild des Reisenden mit einer Kamera aufgenommen. Über eine entsprechende Gesichtserkennungssoftware wird dieses Bild mit dem im Chip des Passes gespeicherten Lichtbild verglichen. Parallel wird die Echtheit des Ausweises geprüft. Erfolgt insgesamt keine Beanstandung durch das System, öffnet sich eine Schleuse und der Reisende kann die Grenze übertreten. Beamte der Bundespolizei überwachen den Prozess und können bei Bedarf eingreifen. Ebenso entscheiden sie, ob und welche zusätzlichen Kontrollfolgemaßnahmen erforderlich sind.

Ziel des Verfahrens ist es, das Grenzkontrollpersonal bei der Überprüfung der Reisenden zu unterstützen, die Grenzkontrolle zu beschleunigen und damit Wartezeiten zu vermeiden.

Ich begrüße es, dass EasyPASS – im Gegensatz zu ABG – keine vorherige Registrierung des Passagiers erfordert. Des Weiteren werden keine Daten der Personen über einen unbegrenzten Zeitraum in einer Datenbank gespeichert, um den automatisierten Grenzkontrollprozess nutzen zu können. Damit werden auch keine Begehrlichkeiten geweckt, die biometrischen Daten anderweitig zu nutzen.

Ob das ABG-Verfahren, nachdem der Erfolg von EasyPASS erkennbar ist, beendet wird, bleibt abzuwarten. Die bei ABG bestehenden Rahmenbedingungen für Vielflieger (z. B. die Registrierung) können auch im EasyPASS-Verfahren angewendet werden.

Ich habe das Projekt EasyPASS und die erforderlichen Tests begleitet und werde es weiterhin beobachten (vgl. Nr. 7.3.2).

Im Jahre 2010 wurde die Testphase beendet und das Verfahren zur Nutzung freigegeben. Es ist geplant, das Verfahren auch auf anderen Flughäfen einzusetzen.

### 3.6 Kein Überflieger: ELSTER-Online

*Die Evaluierung des ELSTER-Online Verfahrens ist unzureichend. Vor einer dauerhaften Zulassung des Verfahrens müssen die Belange des Datenschutzes und der IT-Datensicherheit gewährleistet sein.*

Die Finanzverwaltung stellt den Steuerpflichtigen zur elektronischen Übermittlung von Dokumenten (z. B. bei der Abgabe einer Steuererklärung) das ELSTER-Online Verfahren als Kommunikationsportal zur Verfügung. Entspre-

chend des gesetzgeberischen Auftrags wurde das Verfahren evaluiert, was ich zum Anlass für einen Beratungs- und Informationsbesuch beim Bundesministerium der Finanzen (BMF) genommen habe. Das vorgelegte Ergebnis wird den Anforderungen an eine umfassende und vollumfängliche Evaluierung des ELSTER-Online Verfahrens, bei dem auf den Einsatz der qualifizierten elektronischen Signatur verzichtet wird, allerdings nicht gerecht. Insbesondere wegen der Diskussion um eine dauerhafte Zulassung des derzeit noch befristet bis zum 31. Dezember 2011 zugelassenen „anderen sicheren Verfahrens“ (ELSTER-Online) nach § 87a Absatz 6 AO wäre eine weitergehende Analyse seiner Risiken und Schwachstellen erforderlich gewesen.

Seit Inbetriebnahme von ELSTER-Online hat sich die Bedrohungslage deutlich geändert, z. B. durch zunehmendes Angriffspotential von Trojanern. Außerdem hätten Alternativen zum derzeit praktizierten Verfahren näher untersucht werden müssen, wozu etwa die Nutzung des elektronischen Identitätsnachweises (eID) des neuen Personalausweises zählt (vgl. Nr. 3.2). In rechtlicher Hinsicht setzt sich die Evaluierung nur in Ansätzen mit den unterschiedlichen Rechtsfolgen auseinander, die sich ergeben, je nachdem ob das „andere sichere Verfahren“ oder eine qualifizierte elektronische Signatur verwendet wird.

Weil das BMF überlegt, ELSTER-Online dauerhaft zuzulassen, habe ich meinen Beratungs- und Informationsbesuch genutzt, um die maßgeblichen datenschutzrechtlichen Anforderungen an die Ausgestaltung des „anderen sicheren Verfahrens“ nach § 87a Absatz 6 AO zu erörtern. Dazu zählen insbesondere die folgenden Punkte:

- Ausgehend von der gesetzlichen Grundlage des § 87a Absatz 6 AO soll das „andere sichere Verfahren“ *neben* der qualifizierten elektronischen Signatur Anwendung finden. Allen Steuerpflichtigen sollte daher zumindest die Möglichkeit eröffnet werden, ihre Kommunikation mit der Finanzverwaltung auch durch die elektronische Signatur sichern zu können. Diese Möglichkeit besteht – entgegen der ausdrücklichen gesetzlichen Vorgaben – bislang nicht.

- Die Gebote der Transparenz und Normenklarheit erfordern eine gesetzliche Präzisierung dahingehend, dass das „andere sichere Verfahren“ der qualifizierten elektronischen Signatur nicht gleich gestellt ist und nur eine geringere Sicherheit als diese bietet.

- Ich halte eine gesetzliche Regelung der Rechtsfolgen für erforderlich, die an die Verwendung des „anderen sicheren Verfahrens“ geknüpft sind. Dies betrifft u. a. spezifische Regelungen zur Zuordnung der übermittelten Dokumente oder zur Beweislastverteilung, die insbesondere bei Beteiligung Dritter (z. B. Steuerberater) problematisch sein können.

- In technisch-organisatorischer Hinsicht wäre durch die Finanzverwaltung zu prüfen, inwieweit die fortgeschrittene elektronische Signatur beim ELSTER-Online Verfahren zur Anwendung kommen könnte. ELSTER-Online autorisiert derzeit zwar den Absender einer Nachricht, dagegen wird zur Authentizität und Integrität der übermittelten Dokumente (z. B. der Steuererklärung) keine Aussage getroffen. Die Anwendung der fortgeschrittenen elektronischen Signatur könnte diesbezüglich Abhilfe schaffen.

Eine Antwort des BMF auf meine Vorschläge lag bei Redaktionsschluss noch nicht vor.

## 4 Internet

### 4.1 Die Lokalisierung des Einzelnen – Geodaten und Persönlichkeitsrechte

*Erwartungsgemäß (vgl. 22. TB Nr. 7.1) hat die Bedeutung von Geoinformationen enorm zugenommen – mit erheblichen Auswirkungen auf das Persönlichkeitsrecht. Besonders brisant ist die Kombination von Geodaten mit Internetdiensten.*

Auf Seiten der Betroffenen führt vor allem die massenhafte Durchsetzung von Smartphones dazu, dass unzählige Dienste angeboten werden, die auch eine Verarbeitung von Lokalisierungsdaten erfordern oder solche Daten jedenfalls verwenden. Durch die permanente Verknüpfung des Aufenthaltsortes mit weiteren Informationen über den Betroffenen entsteht eine völlig neue Dimension der Profilbildung (vgl. dazu Nr. 6.2).

Für reichlichen Gesprächsstoff sorgte der von Google nun auch in Deutschland eingeführte Dienst Street View. Neben der Bearbeitung einer außerordentlich hohen Zahl von Eingaben und Anfragen zu diesem Thema lag der Schwerpunkt meiner Arbeit hier insbesondere darin, mit den betroffenen Branchen und der Politik darüber zu diskutieren, ob und wie weit das Verhältnis zwischen der Verarbeitung georeferenzierter Informationen und den Persönlichkeitsrechten der von dieser Verarbeitung Betroffenen neu justiert werden muss (vgl. Nr. 4.1.1).

Die Debatten nahmen noch zu, als bekannt wurde, dass Google im Rahmen der Kamerafahrten nicht nur Bildaufnahmen anfertigte, sondern auch Daten von WLAN-Netzen erfasst hat (vgl. Nr. 4.1.2).

Die öffentliche Debatte über Google Street View hat schließlich dazu geführt, dass auf der politischen Ebene über gesetzgeberischen Handlungsbedarf beim Umgang mit personenbezogenen Geoinformationen nachgedacht wird. Die Internetwirtschaft hat hierzu einen Geodaten-Kodex vorgelegt; das BMI plant die Einführung einiger grundsätzlicher gesetzlicher Regelungen (vgl. Nr. 4.1.3).

Nicht nur die Privatwirtschaft erhebt, verarbeitet und nutzt in immer stärkerem Maße personenbezogene Geodaten, auch die öffentliche Verwaltung ist zur Erfüllung ihrer Aufgaben seit jeher an Geoinformationen interessiert. Auch in diesem Bereich führen die Möglichkeiten der Informationstechnik zu einer stärkeren persönlichkeitsrechtlichen Relevanz (vgl. Nr. 4.1.4).

### 4.1.1 Mein Haus im Internet: Google Street View und andere Dienste

*Niemand kann sich dem Internet mehr vollständig entziehen. Diese Erfahrung machten jedenfalls viele Mieter und Hauseigentümer.*

Bereits in meinem letzten Tätigkeitsbericht (22. TB Nr. 7.2) habe ich den vom Unternehmen Google geplanten Dienst Street View ausführlich dargestellt, dessen Auswirkungen auf das Persönlichkeitsrecht beschrieben und daraus datenschutzrechtliche Forderungen abgeleitet. Dabei werden Digitalfotos von Häuserfassaden und Grundstücken ins Internet gestellt und ermöglichen dem Nutzer virtuelle Rundgänge. Datenschutzrechtlich problematisch ist dabei zum einen, dass die Informationen durch das Unternehmen aber auch von jedem beliebigen Internetnutzer mit weiteren Informationen über Bewohner und Eigentümer der gezeigten Grundstücke zusammengeführt werden können. Street View und ähnliche Dienste sind somit eine weitere Quelle für immer umfangreichere und aussagekräftigere Persönlichkeitsprofile (vgl. Nr. 1, 4.1.3, 6.2).

Inzwischen hat Google auch in Deutschland umfangreiches digitales Bildmaterial erfasst und seinen Dienst für deutsche Städte freigeschaltet; andere Unternehmen bieten ähnliche Dienste an. Es hat sich aber auch gezeigt, dass viele Grundstückseigentümer und Bewohner die flächendeckende Abbildung der Straßenansichten mit Sorge betrachten. So führte bereits die Ankündigung der Inbetriebnahme des Dienstes zu intensiven Diskussionen in der Öffentlichkeit. Auch die vergleichsweise hohe Zahl von Eingaben, die allein mich zu dieser Thematik erreicht haben, obwohl der BfDI nicht einmal die zuständige Aufsichtsbehörde ist, unterstreicht die Besorgnis vieler Bürgerinnen und Bürger.

In intensiven Gesprächen haben der zuständige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit sowie Vertreter anderer Aufsichtsbehörden erreichen können, dass Google zugesagt hat, den in meinem letzten Tätigkeitsbericht beschriebenen Forderungen (22. TB Kasten zu Nr. 7.2) weitgehend nachzukommen. Das Unternehmen hat gegenüber dem Hamburgischen Beauftragten die Einhaltung von 13 Punkten zugesichert (vgl. Kasten zu Nr. 4.1.1). Die wichtigsten Zusagen beziehen sich dabei zum einen auf die vor Veröffentlichung zu erfolgende automatisierte Verschleierung von Gesichtern und Kfz-Kennzeichen sowie auf die Möglichkeit der Betroffenen, sowohl vor als auch nach Veröffentlichung der Bilder der Verbreitung ihrer personenbezogenen Daten widersprechen zu können. Diese Zusagen entsprechen den Anforderungen des Bundesdatenschutzgesetzes.

Bedauerlich ist, dass trotz intensiver Abstimmung mit den Datenschutzbehörden in Europa ein gleichwertiger Schutz der Persönlichkeitsrechte in der Mehrzahl der betroffenen europäischen Länder bislang nicht erreicht werden konnte. Dies unterstreicht die Notwendigkeit, im Rahmen der grundlegenden Überarbeitung des europäischen Datenschutzrechts (vgl. Nr. 13.2) dessen Anwendbarkeit auch für solche Dienste sicherzustellen, die von außereuropäischen Anbietern auf dem europäischen Markt angeboten werden und bei denen Daten der hier wohnenden Menschen betroffen sind.

Während für die nach Veröffentlichung im Internet bestehende Widerspruchsmöglichkeit bereits technische Verfahren existierten, musste Google für den Vorab-Widerspruch eine neue technische Lösung entwickeln, um einerseits die Widersprüche möglichst schnell bearbeiten und andererseits die eingelegten Widersprüche den Bildaufnahmen eindeutig zuordnen zu können. Außerdem sollte das missbräuchliche Einlegen von Vorab-Widersprüchen weitgehend verhindert werden.

Im Ergebnis wurde eine Lösung gefunden, die für Street View überwiegend positive Resultate erzielte, aber auch grundsätzliche Probleme aufwarf. Der Vorab-Widerspruch basiert darauf, dass die Betroffenen über ein Online-Tool, das in den bereits verfügbaren Kartendienst des Unternehmens eingebaut ist, den Punkt markieren können, auf den sich ihr Widerspruch bezieht. Sofern damit eine eindeutige Zuordnung zu konkreten Aufnahmen möglich war, bekam der Betroffene einen Verifizierungscode postalisch zugesandt und konnte mit dessen Hilfe wiederum online das Widerspruchsverfahren abschließen. Zum Ende des Jahres 2010 hat Google schließlich zunächst für die 20 größten Städte Deutschlands den Dienst Street View mit der Veröffentlichung der Straßenansichten gestartet.

Problematisch am Verfahren des Vorab-Widerspruchs ist, dass Google auf diese Weise zusätzliche personenbezogene Daten der Betroffenen erhält, deren Verwendung durch die Aufsichtsbehörde nur schwer kontrolliert werden kann. Dabei handelte es sich neben Namen und Anschriften der Betroffenen auch um die konkrete Beschreibung eines Hauses oder Grundstücks. Wie zahlreiche Eingaben zeigten, hat dies viele Betroffene davon abgehalten, Widerspruch einzulegen: das Vertrauen, dass Google mit ihren im Rahmen des Widerspruchs angegebenen Daten sorgfältig umgeht, ist offenbar gering.

Um eine möglichst datenschutzfreundliche Inanspruchnahme des Widerspruchsrechts zu gewährleisten, habe ich daher die Einführung eines zentralen Widerspruchsregisters bei einer vertrauenswürdigen Stelle angeregt (vgl. Nr. 4.2).

Kasten zu Nr. 4.1.1

**13 Zusagen von Google zum Internetdienst Google Street View**

Die folgenden Punkte sind zusammengestellt aus bereits in dem Dienst enthaltenen Maßnahmen, Zusagen gegenüber dem Düsseldorfer Kreis im April 2009 und gegenüber dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit im Juni 2009:

1. Google hat verbindlich zugesichert, eine Technologie zur Verschleierung von Gesichtern vor der Veröffentlichung von derartigen Aufnahmen einzusetzen.
2. Google hat verbindlich zugesichert, eine Technologie zur Verschleierung von Kfz-Kennzeichen vor der Veröffentlichung derartiger Aufnahmen einzusetzen.
3. Google hat verbindlich zugesichert, Widerspruchsmöglichkeiten zur Entfernung bzw. Unkenntlichmachung eines Gebäudes durch einen Bewohner oder Eigentümer vorzuhalten und derartige Widersprüche zu bearbeiten.
4. Google hat verbindlich zugesichert, dass Widersprüche zu Personen, Kennzeichen und Gebäuden bzw. Grundstücken bereits vor der Veröffentlichung von Bildern in einer einfachen Form berücksichtigt werden mit der Folge, dass die entsprechenden Bilder vor der Veröffentlichung unkenntlich gemacht werden. Voraussetzung ist eine Identifizierung des Grundstücks, der Person oder des Fahrzeugs.
5. Google hat verbindlich zugesichert, die geplanten Befahrungen mit einem Hinweis auf die Widerspruchsmöglichkeit im Internet rechtzeitig vorher bekannt zu geben. Die vorhandenen Befahrungspläne werden bis zu zwei Monate im Voraus veröffentlicht und ständig aktualisiert. Google hat die verbindliche Zusage gemacht, die Liste genauer zu gestalten und auf Landkreise und kreisfreie Städte zu erstrecken. Die kreisfreien Städte wurden bereits eingepflegt, die Landkreise sollen nach Auskunft von Google bis etwa Mitte Juli 2009 eingestellt werden.
6. Google hat verbindlich zugesagt, dass die Widerspruchsmöglichkeit auch nach der Veröffentlichung noch besteht.
7. Die Rohdaten werden nach Aussage von Google zum Zwecke der Weiterentwicklung und Verbesserung der von Google entwickelten Technologie zur Unkenntlichmachung von Gesichtern, Kfz-Kennzeichen und Gebäudeansichten benötigt. Google hat verbindlich zugesichert, die Löschung/Unkenntlichmachung der Rohdaten vorzunehmen, indem die Ergebnisse aus dem Prozess zur Unkenntlichmachung von Gesichtern und Kfz-Kennzeichen in die Rohdaten übernommen werden, sobald die Speicherung und Verarbeitung der Rohdaten nicht mehr für die genannten Zwecke erforderlich ist.
8. Google hat verbindlich zugesichert, die Löschung oder Unkenntlichmachung der Rohdaten von Personen, Kfz und Gebäudeansichten vorzunehmen, die aufgrund eines Widerspruchs zu entfernen sind. Die Löschung oder Unkenntlichmachung dieser Daten in den Rohdaten wird bereits vor der Veröffentlichung vorgenommen, wenn der Widerspruch bis zu einem Monat vor Veröffentlichung der Bilder bei Google eingeht. Später oder auch nach Veröffentlichung eingehende Widersprüche führen zu einer Löschung in den Rohdaten binnen zwei Monaten.
9. Google hat die Erstellung eines Verfahrensverzeichnisses zugesichert.
10. Im Falle von Verknüpfungen des Dienstes durch andere Anbieter behält sich Google in den Nutzungsbedingungen das Recht vor, bei offensichtlicher Verletzung anwendbarer Gesetze, die Schnittstelle zu unterbinden.
11. Google hat zugesichert, eine Beschreibung der Datenverarbeitungsprozesse und der technischen und organisatorischen Maßnahmen für Google Street View vorzulegen. Insbesondere gehört hierzu auch eine deutliche Beschreibung des Umgangs mit den Widersprechendendaten von der Entgegennahme des Widerspruchs bis zur endgültigen Löschung bzw. Unkenntlichmachung.
12. Widerspruch kann eingelegt werden im Internet unter www.google.de/streetview oder schriftlich bei der Google Germany GmbH, betr.: Street View, ABC-Straße 19, 20354 Hamburg. Der Link mit dem Text: „FAQ Street View (inkl. Widerspruchsmöglichkeiten)“ ist nunmehr direkt auf der ersten Seite der Hilfeseiten für Google Maps Deutschland erreichbar. Diese Hilfeseiten erreicht jeder Nutzer direkt aus dem Produkt Google Maps Deutschland, wenn er oben rechts den Link „Hilfe“ klickt.
13. Die bei Google eingelegten Widersprüche werden zeitnah bestätigt. E-Mails mit Widersprüchen werden bereits bestätigt, alle entsprechenden Briefe werden fortlaufend beantwortet.

### 4.1.2 Erfassung von WLAN-Netzen und übertragenen Inhalten

*Die Kamerafahrzeuge von Google fertigten nicht nur digitale Fotos von Gebäude. Sie erfassten auch Daten privater Funknetze. Die zuständigen Datenschutzbehörden, die Betroffenen und die Öffentlichkeit wurden darüber nicht informiert.*

Im Rahmen der Diskussionen um Google Street View (vgl. o. Nr. 4.1.1) wurde bekannt, dass die Kameraautos des Unternehmens neben den Hausfassaden auch Informationen von privaten und öffentlichen WLAN-Netzen erfasst, gespeichert und zur weiteren Verarbeitung in die USA übermittelt haben. Pikant ist dabei, dass die Erfassung der WLAN-Daten erfolgte, ohne dass die zuständigen Datenschutzbehörden, die Betroffenen oder die Öffentlichkeit davon informiert wurden. Erst nachdem eine ausländische Datenschutzbehörde dies bei der Prüfung eines von Google ausgesandten Kamerafahrzeugs festgestellt hatte und diese Feststellung öffentlich wurde, bestätigte Google den Sachverhalt.

Das Unternehmen rechtfertigte die Datenerhebung damit, es habe die Standorte der WLAN-Netzes erhoben, um diese Geoinformationen später zur Bereitstellung von Ortungsdiensten (vgl. hierzu Nr. 6.2) zu verwenden.

Die Rechtmäßigkeit des „WLAN-Scannings“ ist umstritten, da es sich bei den erhobenen Daten teilweise auch um personenbeziehbare Informationen handelt. So werden in dem Datensatz zu einem WLAN-Netz unter anderem die eindeutige MAC-Adresse des WLAN-Routers, die SSID (die frei wählbare Bezeichnung des WLAN-Netzes), die Feldstärke des Signals sowie die Information, ob es sich um ein verschlüsseltes oder unverschlüsseltes Netz handelt, erfasst. Gerade bei der SSID, bei der einige Netzwerkbetreiber ihren Namen und teilweise sogar ihre Adressdaten angeben, kann es sich um ein Datum mit eindeutigem Personenbezug handeln. Aber auch die MAC-Adresse im Zusammenhang mit den Geokoordinaten des Standortes und der Feldstärke ist geeignet, ein WLAN-Netz einer ganz konkreten Adresse zuzuordnen. Gerade in nicht so stark besiedelten Gebieten weist ein erfasstes WLAN-Netz Personenbezug auf. Gemeinsam mit meinen europäischen Kollegen bin ich daher der Auffassung, dass ein „WLAN-Scanning“ die Einwilligung der erfassten WLAN-Netzbetreiber erfordert.

Unter keinen Umständen dürfen aber „Payload-Data“, also Inhaltsdaten, die über das WLAN-Netz verschickt und empfangen werden, erhoben werden. Solche Daten, die von den WLAN-Scannern immer dann miterfasst werden können, wenn das Netz nicht durch eine Verschlüsselung gesichert wurde, fallen unter das Fernmeldegeheimnis und unterliegen dem Schutz des Grundgesetzes. Eine heimliche Erhebung derartiger Informationen ist somit grundsätzlich strafrechtlich sanktionierbar.

Nachdem Google zunächst abgestritten hatte, derartige Inhaltsdaten aus WLAN-Netzen zu erheben, haben Datenschutzbehörden festgestellt, dass sehr wohl, und zwar in erheblichem Umfang, entsprechende Daten erfasst und gespeichert wurden. Die gespeicherten Daten umfassten z. T. Kennungen, Passwörter und andere sensible Informationen. Erneut bestätigte das Unternehmen erst im Anschluss an diese Feststellungen den Sachverhalt und entschuldigte sich öffentlich für die heimliche Erhebung.

In dieser Angelegenheit hat die Staatsanwaltschaft in Hamburg ein Ermittlungsverfahren gegen Google eingeleitet.

Ich halte es für skandalös, wie der weltweit führende Internetkonzern hier agiert hat. Offenbar war er der Auffassung, dass die ansonsten von ihm propagierte Offenheit und Datentransparenz nicht für die eigenen Praktiken gilt.

### 4.1.3 Selbstregulierung oder Gesetz? – Ein neuer Rechtsrahmen für Geodatendienste

*Beim Datenschutz für Internetdienste setzt der Bundesinnenminister auf die Selbstregulierung der Wirtschaft. Der Gesetzgeber soll sich auf die Formulierung „roter Linien“ beschränken. Zweifel sind angebracht, ob damit den Datenschutzerfordernissen ausreichend Rechnung getragen werden kann.*

Auf die anhaltenden öffentlichen Diskussionen über den Dienst Street View (vgl. Nr. 4.1.1) hat die Bundesregierung mit politischen Aktivitäten reagiert. In einem Spitzengespräch mit Vertretern aus Wirtschaft, Politik, Datenschutzbehörden und Verwaltung am 20. September 2010 (vgl. a. Nr. 1) hat der Bundesminister des Innern vorgeschlagen, die Internetwirtschaft solle im Wege der Selbstregulierung einen Datenschutz-Kodex zum Umgang mit personenbezogenen Geoinformationen vorlegen und mit den Datenschutzbehörden abstimmen. Sofern dieser Kodex bestimmte Bedingungen erfülle, könne sich der Gesetzgeber nach Ansicht des BMI darauf beschränken, als eine „rote Linie“ die Mindestbedingungen für den Umgang mit solchen Daten festzulegen, um schwerwiegende Beeinträchtigungen des Persönlichkeitsrechts zu unterbinden. Insbesondere sei ein allgemeines Widerspruchsrecht gegen die Veröffentlichung personenbezogener Daten im Internet nicht erforderlich.

Ich stehe – ebenso wie meine Kollegen in den Ländern – einem solchen Ansatz skeptisch gegenüber. Ich sehe den Gesetzgeber in der Pflicht, selbst für einen angemessenen Schutz des Persönlichkeitsrechts im Internet und damit auch beim Umgang mit personenbezogenen Geodaten zu sorgen. Hierzu gehört auch die Einführung eines allgemeinen Widerspruchsrechts gegen eine Veröffentlichung personenbezogener Daten im Internet.

Sofern an dem Regelungsmodell festgehalten werden soll, muss ein Datenschutz-Kodex einige Mindestanforderungen wie das allgemeine Widerspruchsrecht berücksichtigen. Vor allem muss ein solcher Kodex für alle Unternehmen verbindlich sein und von den Aufsichtsbehörden auch durchgesetzt werden können (vgl. Kasten zu Nr. 4.1.3).

Der Branchenverband BITKOM hat am 1. Dezember 2010 den Entwurf eines Geodaten-Kodexes vorgelegt. Am gleichen Tage hat der Bundesminister des Innern seine Vorstellungen eines Gesetzes über die Mindestanforderungen („rote Linie“) öffentlich bekanntgegeben. Der Entwurf von BITKOM beschränkt sich auf die Veröffentlichung von Panoramaaufnahmen, gilt also nicht allgemein für die Veröffentlichung personenbezogener Daten im Internet. Er sieht ein allgemeines Widerspruchsrecht nach der Veröffentlichung von Bildern sowie die Einrichtung eines zentralen Portals vor, das für die Einlegung der Widersprüche genutzt werden kann. Die Möglichkeit des Vorab-Widerspruchs ist bislang nicht berücksichtigt. Der Entwurf enthält Sanktionen für Verstöße gegen den Kodex, ist aber nur für dessen Unterzeichner verbindlich.

Die Vorschläge des BMI zielen – anders als der Entwurf von BITKOM – auch auf andere Internetdienste ab, beschränken sich allerdings auf schwerwiegende Eingriffe in das Persönlichkeitsrecht. Demnach sollen (nur) solche Veröffentlichungen personenbezogener Daten im Internet unzulässig sein, die einen besonders schwerwiegenden Eingriff darstellen, z. B. Daten, aus denen sich umfangreiche Persönlichkeits- oder Bewegungsprofile ergeben können, ehrverletzende Informationen oder andere besonders

sensitive Daten. Die Pressefreiheit solle dabei geschützt werden.

Die Datenschutzbeauftragten in Bund und Ländern waren an der Ausarbeitung der Vorschläge bisher noch nicht beteiligt. BITKOM hat für Anfang 2011 einen Abstimmungsprozess mit den Aufsichtsbehörden eingeleitet. Ich werde die Vorschläge gemeinsam mit meinen Kollegen in den Ländern eingehend prüfen und den Prozess konstruktiv begleiten.

Unabhängig vom weiteren Fortgang der Diskussionen ist festzustellen, dass insbesondere der Entwurf des Geodaten-Kodex einige positive Ansätze enthält, insgesamt aber bisher hinter den Forderungen der Datenschutzbeauftragten in Bund und Ländern zurückbleibt:

So sieht der Entwurf des Kodexes zwar ein allgemeines Widerspruchsrecht gegen eine Veröffentlichung vor, beschränkt dieses aber auf den nachträglichen Widerspruch. Eine effektive Durchsetzung der Persönlichkeitsrechte wäre jedoch nur mit einem Vorab-Widerspruch zu erreichen. Daten, die einmal im Netz sind, lassen sich nur schwer wieder zurückholen. Ebenso greift die bloße Einrichtung eines Portals zur Koordinierung der Widerspruchsverfahren einzelner Anbieter noch zu kurz und setzt die Forderungen nach einem Widerspruchsregister nur zu einem kleinen Teil um. Auch die Verbindlichkeit des Datenschutz-Kodexes müsste erheblich verbessert werden. Das Bundesdatenschutzgesetz sieht in § 38a die Einführung verbindlicher Verhaltensregeln vor; dieses Verfahren sollte auch genutzt werden. Schließlich wird die internationale Dimension der Thematik in den Vorschlägen bisher gar nicht berücksichtigt. Es muss – ggf. durch Änderung des europäischen Rechtsrahmens (vgl. Nr. 13.2) – sichergestellt werden, dass Anbieter, die auf dem europäischen Markt tätig sind und personenbezogene Daten der in Europa lebenden Bürgerinnen und Bürger verarbeiten, auch die Regeln des europäischen Datenschutzrechts beachten müssen. Die Anknüpfung an eine Niederlassung in Europa oder die Nutzung von in Europa belegenen Mitteln der Datenverarbeitung ist unzureichend, da viele bedeutende Konzerne im Internetbereich hiervon nicht erfasst werden.

Die vom BMI angekündigten Änderungen des BDSG („rote Linie-Gesetz“) sind indes – zumindest im Hinblick auf die Frage der Bildung von Persönlichkeitsprofilen – völlig unzureichend. Schon heute ist es unzulässig, umfassende und systematisch erstellte Persönlichkeitsprofile ohne gesetzliche Grundlage und ohne Einwilligung des Betroffenen zu veröffentlichen, da eine solche Veröffentlichung überwiegende schutzwürdige Belange des Betroffenen verletzen und damit gegen § 28 BDSG verstoßen würde. Eine entsprechende Regelung, die sich auf die Veröffentlichung von Persönlichkeitsprofilen beschränkt, würde den Datenschutz im Internet nicht verbessern. Notwendig wäre hingegen ein Verbot der Bildung von Persönlichkeitsprofilen. Ein solches Verbot will das BMI aber bisher nicht.

Es bleibt abzuwarten, ob die Bundesregierung den angekündigten „rote Linie“-Gesetzentwurf vorlegen wird und wie Bundestag und Bundesrat damit umgehen werden.

Kasten zu Nr. 4.1.3

**Moderner Datenschutz im Internet – ein erster Schritt**

Gemeinsame Erklärung des Landesbeauftragten für Datenschutz und Nordrhein-Westfalen, des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 22. September 2010

An dem vom Bundesminister des Innern, Dr. Thomas de Maizière, initiierten Spitzengespräch zum Thema Digitalisierung von Stadt und Land am 20. September 2010 haben der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Herr Ulrich Lepper als Vorsitzender des Düsseldorfer Kreises der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Herr Prof. Dr. Johannes Caspar, als für einige wichtige Internetunternehmen zuständige Aufsichtsbehörde sowie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, teilgenommen. Sie geben hierzu folgende gemeinsame Erklärung ab:

1. Das Spitzengespräch hat die Bedeutung des Datenschutzes beim Umgang mit Geoinformationen, aber auch allgemein bei Internetdiensten eindrucksvoll unterstrichen. Die enorme Vielfalt der Angebote steht dabei in einem auffälligen Missverhältnis zu den unklaren und unzureichenden rechtlichen Rahmenbedingungen zur Wahrung der Persönlichkeitsrechte. Wir halten eine Regulierung im Sinne klarer und verbindlicher Anforderungen zum Schutz der Privatsphäre daher für dringend erforderlich.
2. Regelungen zum Umgang mit Geoinformationen können nur ein erster Schritt zur Modernisierung des Datenschutzes im Internet sein.
3. Der Staat ist verpflichtet, auch im Bereich der Privatwirtschaft für einen angemessenen Schutz des Grundrechts auf informationelle Selbstbestimmung zu sorgen. Die hierzu notwendigen wesentlichen Maßnahmen sind unmittelbar in einem Gesetz zu regeln. Hierzu gehört auch ein allgemeines Widerspruchsrecht der Betroffenen gegen die Veröffentlichung ihrer Daten im Internet.

4. Wir sehen es positiv, dass der Bundesminister des Innern eine gesetzliche Regelung anstrebt, die als rote Linie die unabdingbaren Mindestanforderungen für die Verarbeitung von personenbezogenen Geoinformationen festschreibt. Diese muss aber einen angemessenen Schutz des Rechts auf informationelle Selbstbestimmung gewährleisten. Eine Selbstverpflichtung der Internetwirtschaft (Datenschutzkodex für Geodienste) kann gesetzliche Regelungen nicht ersetzen. Soweit die Bundesregierung gleichwohl diesen Weg einschlagen will, muss eine Selbstverpflichtung mindestens die folgenden Anforderungen erfüllen:
   a. Es ist ein allgemeines Widerspruchsrecht gegen die Veröffentlichung georeferenzierter personenbezogener Informationen im Internet zu schaffen.
   b. Um das Einlegen von Widersprüchen möglichst unbürokratisch zu ermöglichen und die Daten der Widersprechenden optimal zu schützen, ist ein Widerspruchsregister einzurichten. Dieses ist bei einem unabhängigen Trust Center als vertrauenswürdiger Stelle zu führen.
   c. Die Selbstverpflichtung muss für die gesamte Internetwirtschaft verbindlich sein.
   d. Bei Verstößen gegen die Selbstverpflichtung müssen wirksame Sanktionen vorgesehen werden.
   e. Der Datenschutz-Kodex darf keinesfalls hinter den Verhandlungsergebnissen zurückbleiben, die die zuständigen Aufsichtsbehörden mit den Anbietern einschlägiger Dienste (insbesondere Google Street View) erreicht haben.
5. Sofern es der Internetwirtschaft bis zum 5. IT-Gipfel am 7. Dezember 2010 nicht gelingt, eine Selbstverpflichtung vorzulegen, die den genannten Anforderungen genügt, muss der Gesetzgeber entsprechende Regelungen schaffen.

### 4.1.4 Geodaten im öffentlichen Bereich

*Auch die von öffentlichen Stellen gesammelten Geodaten können Persönlichkeitsverletzungen bewirken.*

Auch die öffentliche Verwaltung ist, z. B. zu Zwecken der Daseinsvorsorge oder zu planerischen oder statistischen Zwecken, in einem erheblichen Umfang auf die Verarbeitung von Geoinformationen angewiesen. Außerdem gehört es zu den Aufgaben einer Reihe von Behörden, selbst für Zwecke der behördlichen oder wirtschaftlichen Weiterverwendung Geoinformationen zu erheben und bereitzustellen. Hierzu gehören in erster Linie die sog. Geobasisdaten (vgl. Kasten zu Nr. 4.1.4), aber auch detaillierte Geofachdaten.

In Umsetzung der INSPIRE-Richtlinie haben der Bund und die meisten Länder Geodatenzugangsgesetze erlassen, die die Einrichtung einer nationalen und europaweiten Geodateninfrastruktur und ein allgemeines Zugangsrecht zu Geodaten vorsehen (vgl. 22. TB Nr. 7.1).

Für den Umgang mit Geobasisdaten durch geodatenhaltende Stellen des Bundes plant die Bundesregierung die Vorlage eines Entwurfs für ein Bundesgeobasisdatengesetz. Der Gesetzentwurf des BMI befindet sich in der Abstimmung mit den anderen Ressorts, an der ich ebenfalls beteiligt werde.

Den datenschutzrechtlichen Kern der Diskussion bildet die Frage, in welchem Umfang Geodaten personenbezogen sind. Nur bei Personenbezug ist das Datenschutzrecht anwendbar und kann den Einzelnen schützen. Unbestritten ist, dass es gerade bei den Geobasisdaten eine Reihe von Verwendungsmöglichkeiten gibt, die nur geringe Relevanz für die Persönlichkeitsrechte aufweisen. Vereinzelt wird vorgeschlagen, bei solchen eher sachbezogenen Informationen von vornherein dann nicht von einem Personenbezug auszugehen, wenn eine Herstellung des Personenbezugs nicht bezweckt wird. Ich halte die Orientierung am Verwendungszweck für einen gefährlichen und rechtlich falschen Ansatz. Nach dem Volkszählungsurteil des Bundesverfassungsgerichts gibt es keine belanglosen Daten. Entscheidend ist allein, ob der Personenbezug gegeben ist oder ohne unverhältnismäßigen Aufwand hergestellt werden kann. Die Herausnahme vermeintlich unsensibler Daten aus dem Anwendungsbereich des Datenschutzrechts hätte fatale Wirkungen: Zum einen könnten diese Daten in einem anderen Verwendungskontext durchaus Auswirkungen auf das Persönlichkeitsrecht haben. Zum anderen ist zu befürchten, dass nicht nur amtliche Geodaten, sondern alle möglichen anderen Daten, die in bestimmten Konstellationen ebenfalls einen nur indirekten Personenbezug aufweisen (IP-Adressen, Telefonnummern, Autokennzeichen), nicht mehr geschützt würden.

Im Hinblick auf die nur geringe Wahrscheinlichkeit und Intensität von möglichen Persönlichkeitsrechtsverletzungen halte ich es für einen besseren Weg, für bestimmte Verwendungen von Daten Erleichterungen vorzusehen, wie es durch das Geodatenzugangsgesetz des Bundes bereits – wenn auch sehr weitgehend – geschehen ist. Der Entwurf des Bundesgeobasisdatengesetzes geht wegen der ungeklärten Fragen der persönlichkeitsrechtlichen Relevanz von Geobasisdaten bisher nicht auf diese Fragen ein, sondern überlässt die Lösung datenschutzrechtlicher Probleme dem allgemeinen Datenschutzrecht.

Kasten zu Nr. 4.1.4

**Stichwort Geodaten:**

**Geobasisdaten** sind diejenigen Geodaten, die die Geotopographie anwendungsneutral in einem einheitlichen geodätischen Referenzsystem beschreiben. Sie sind die Grundlage für Fachanwendungen mit Raumbezug. Zu den Geobasisdaten gehören Landschaft und die Liegenschaften jeweils verbunden mit einem einheitlichen Koordinatensystem.

**Geofachdaten** sind Geodaten aus einem bestimmten Fachgebiet, deren Raumbezug sich entweder direkt durch Koordinaten oder indirekt durch Bezug auf Geobasisdaten ergibt. Hierzu gehören z. B. raumbezogene Daten über Klima, Bevölkerung, Verkehr, Umwelt usw.

Der **Personenbezug** von Geodaten ist dann gegeben, wenn es sich um punktgenaue, d. h. auf ein bestimmtes Grundstück bezogene Informationen handelt, die eine bestimmte sachliche Aussage (z. B. über Art und Maß der baulichen Nutzung, Hochwassergefährdung oder Verkehrserschließung) treffen. Voraussetzung ist, dass es sich bei dem an einem Grundstück Berechtigten um eine natürliche Person handelt und diese ohne unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft identifiziert werden kann.

## 4.2 Widerspruchsrecht gegen die Veröffentlichung personenbezogener Daten im Internet

*Ein effektiver Datenschutz setzt ein verbrieftes Widerspruchsrecht und unkomplizierte Widerspruchsverfahren gegen die Veröffentlichung personenbezogener Daten im Internet voraus.*

Die Aufnahme von Straßenansichten und deren Veröffentlichung im Internet durch Internet-Geodatendienste (vgl. Nr. 4.1.1) hat einmal mehr verdeutlicht, dass das bestehende Datenschutzrecht keinen ausreichenden Schutz gegen die Veröffentlichung personenbezogener Daten im Internet bietet.

Effektiver Datenschutz setzt ein verbindliches Widerspruchsrecht gegen die Veröffentlichung personenbezogener Daten im Internet voraus. Eine entsprechende gesetzliche Regelung müsste allerdings so formuliert werden, dass damit die durch Artikel 5 GG garantierte Meinungs- und Informationsfreiheit nicht eingeschränkt wird. Es ist die Aufgabe des Gesetzgebers, die wesentlichen Verbraucher- und Datenschutzrechte selbst zu regeln. Der von der Internetbranche im Dezember 2010 (vgl. Nr. 4.1.3) vorgelegte Datenschutz-Kodex kann ein gesetzlich verbrieftes, einklagbares Recht auf Widerspruch nicht ersetzen, sondern nur ergänzenden Charakter haben.

In Bezug auf die Verwendung von Geodaten im Internet – wie sie bei Google Street View diskutiert wird – ist deutlich geworden, dass Widerspruchsrechte durch benutzer- und datenschutzfreundliche Verfahren flankiert werden müssen. Bislang müssen die Betroffenen gegenüber jedem einzelnen Geodatendienst separat Widerspruch einlegen – sofern dieser einen Widerspruch überhaupt zugelassen hat. Dies erfordert in der Summe einen nicht unerheblichen Aufwand sowohl für die Betroffenen als auch für die Diensteanbieter. Die Betroffenen müssen mehrfach – gegenüber allen Diensten – ihren Widerspruch erklären und dabei weitere persönliche Daten preisgeben. Zudem müssen sie sich ständig darüber informieren, ob möglicherweise ein neuer Dienst ihre Daten veröffentlichen will. Die Diensteanbieter müssen den Betroffenen und die jeweiligen Grundstücke identifizieren, was ebenfalls mit erheblichem Aufwand verbunden ist. Schließlich ist es eine zusätzliche Erschwernis für die Betroffenen, wenn die Widerspruchsverfahren nicht einheitlich ausgestaltet sind.

Im Interesse eines effektiven und bürgerfreundlichen Datenschutzes, der den Betroffenen leicht auszuübende und einfach durchzusetzende Rechte an die Hand geben muss, würde ein zentrales Widerspruchsregister, das beispielsweise bei der zu errichtenden Stiftung Datenschutz (vgl. Nr. 2.5) als „Trust-Center“ eingerichtet werden könnte, hier Abhilfe schaffen und sicherstellen, dass ein einziger Widerspruch die Betroffenen gegen die Veröffentlichung ihrer personenbezogenen Daten im Internet umfassend schützt. Jeder Betroffene könnte so durch eine einzige Erklärung Widerspruch gegen die Verwendung seiner personenbezogenen Daten im Internet mit Wirkung gegenüber allen Anbietern vergleichbarer Dienste einlegen. Ein solches Verfahren wäre auch datenschutzfreundlich, denn die Anbieter benötigen zur Umsetzung des Widerspruchs nicht die Identitätsdaten der Betroffenen, sondern lediglich Angaben zu den von Widersprüchen betroffenen Objekten.

Die von der Internetbranche als Teil des im Dezember 2010 vorgelegten Datenschutz-Kodex in Aussicht gestellte zentrale Informations- und Widerspruchsstelle genügt diesen Anforderungen nicht, da der Widerspruch nach wie vor individuell für jeden Anbieter von Geodatendiensten eingelegt werden muss. Ich halte deshalb weiterhin die Einrichtung eines zentralen Widerspruchsregisters gegen die systematische, adressgenau erschließbare Veröffentlichung von Geodaten für vorzugswürdig. Falls Erfahrungen mit einem solchen Register positiv ausfallen, könnte es auf weitere Internetdaten ausgeweitet werden und etwa auch Widersprüche gegen die Aufnahme in Telefon- und Adressverzeichnisse im Internet erfassen.

## 4.3 Unbemerkt: Webanalyseprogramme im Dienste der Website-Anbieter

*Anbieter von Telemedien verwenden Analyseprogramme, um die Gestaltung ihres Angebots zu optimieren. Solche Programme müssen die Datenschutzanforderungen des Telemediengesetzes (TMG) erfüllen und dürfen nicht zur Registrierung des individuellen Nutzerverhaltens dienen.*

Wer im Internet Waren oder Informationen anbietet, möchte gerne wissen, wie sich die Nutzer beim Besuch der Website verhalten, welche Seiten besonders häufig aufgerufen werden, welchen Weg ein Nutzer durch ein Angebot wählt und wo er die Website wieder verlässt. Das ist nicht

anders als in der realen Welt, wo Werbepsychologen sich mit dem Kaufverhalten der Verbraucher beschäftigen und Kaufhäuser ebenso wie kleine Geschäfte ihr Angebot dann so präsentieren, dass es die Kunden anspricht und zum Kauf auffordert oder manchmal auch verführt.

Die digitale Welt im Netz bedient sich elektronischer Mittel, um diese Aufgabe zu lösen, denn die vom Nutzer hinterlassenen digitalen Spuren lassen sich leicht auswerten. Und so gibt es zahlreiche Dienst- und Programmangebote, mit deren Hilfe Website-Anbieter das Nutzerverhalten aufzeichnen und analysieren, um dann mit diesen Erkenntnissen die Gestaltung ihres Angebots zu verbessern (zur Nutzung von Google Analytics durch die gesetzliche Krankenkasse vgl. u. Nr. 4.3.1). Diese Dienste verwenden unterschiedliche Verfahren: In vielen Fällen wird die IP-Adresse verwendet, um die „Bewegung" eines Nutzers innerhalb eines Angebots zu verfolgen, oder es wird ein Cookie gesetzt, um den Nutzer beim nächsten Besuch wiederzuerkennen. Oft geschieht beides – und unbemerkt.

Soweit die Fakten. Ein Blick in das für Internet-Angebote zu beachtende TMG zeigt, dass es für die Erstellung von Nutzungsprofilen sehr enge Vorgaben enthält: die Verwendung von Pseudonymen und die Widerspruchsmöglichkeit des Nutzers. Zur Klarstellung sei gesagt, dass die IP-Adresse ein personenbezogenes Datum ist und kein Pseudonym. Und dass der Nutzer sein Widerspruchsrecht nur dann ausüben kann, wenn er von der Beobachtung überhaupt erfährt und auch ein geeignetes Verfahren vorhanden ist, den Widerspruch zu äußern. Diese Vorgaben sind – soweit mir bekannt – in fast keinem der angebotenen Dienste und Programme umgesetzt.

Der Düsseldorfer Kreis der Datenschutzaufsichtsbehörden hat in einem Beschluss die Anforderungen zusammengefasst, die an Webanalyseprogramme gestellt werden (vgl. Kasten zu Nr. 4.3). Website-Anbieter sollten prüfen, ob die von ihnen eingesetzten Programme diese Anforderungen erfüllen, und ggf. Änderungen vornehmen oder ein anderes Produkt einsetzen. Ich habe diesen Beschluss zum Anlass genommen, die Bundesbehörden noch einmal auf die gesetzlichen Vorgaben hinzuweisen.

Im Übrigen: Die Besuche meiner eigenen Website werden nur anonymisiert ausgewertet, denn die IP-Adressen der Nutzer sind um die letzten beiden Oktette gekürzt.

Kasten zu Nr. 4.3

**Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich**
(Düsseldorfer Kreis am 26./27. November 2009)

**Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten**

Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten der Nutzerinnen und Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass bei Erstellung von Nutzungsprofilen durch Web-Seitenbetreiber die Bestimmungen des Telemediengesetzes (TMG) zu beachten sind. Demnach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes.

Im Einzelnen sind folgende Vorgaben aus dem TMG zu beachten:

- Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen.
- Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.
- Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen.
- Personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.
- Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen (einschließlich einer Geolokalisierung) ist aufgrund der Personenbeziehbarkeit dieser Daten daher nur mit bewusster, eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

Werden pseudonyme Nutzungsprofile durch einen Auftragnehmer erstellt, sind darüber hinaus die Vorgaben des Bundesdatenschutzgesetzes zur Auftragsdatenverarbeitung durch die Anbieter einzuhalten.

### 4.3.1 Nutzung von Webanalysediensten durch gesetzliche Krankenkassen

*Einige gesetzliche Krankenkassen nutzten den Webanalysedienst Google Analytics. Dies begegnete datenschutzrechtlichen Bedenken, denen die betreffenden Kassen Rechnung getragen haben.*

Durch Recherchen auf den Internetseiten der gesetzlichen Krankenkassen habe ich festgestellt, dass eine Vielzahl von Kassen den Webanalysedienst Google Analytics ein-

setzt. Der Einsatz dieses Dienstes zur Analyse des Nutzungsverhaltens war unzulässig, da seine derzeitige Konfiguration eine wirksame Wahrnehmung der Rechte auf Widerspruch, Information und Auskunft sowie Löschung der gespeicherten Daten durch den Betroffenen nicht zuließ (vgl. dazu Nr. 4.3). Ich habe die in meinem Zuständigkeitsbereich liegenden Krankenkassen über meine Rechtsauffassung informiert und gebeten, den Einsatz von Google Analytics umgehend einzustellen und die vorhandenen Daten zu löschen. Die betreffenden Websiteanbieter haben daraufhin erklärt, diesen Webanalysedienst zukünftig nicht mehr zu verwenden. Eine stichprobenartige Überprüfung hat diese Zusagen bestätigt.

### 4.3.2 Immer noch: Der Dissenz bei IP-Adressen

*IP-Adressen sind personenbezogene Daten. Dies wird nicht von allen so gesehen.*

Im Zusammenhang mit meiner Aufsichtstätigkeit im Bereich der Bundesbehörden spielt nicht unwesentlich die „alte“ Frage eine Rolle, ob IP-Adressen personenbezogene Daten sind. Nach Auffassung des BMI und des BSI handelt es sich bei IP-Adressen dann nicht um personenbezogene Daten, wenn sie beim Anbieter einer Website als Nutzungsdaten anfallen. Sie dürften deshalb dort beliebig lange gespeichert und sowohl für Statistik- als auch für Datensicherheitszwecke verwendet werden.

Demgegenüber gehe ich davon aus, dass IP-Adressen – jedenfalls im Regelfall – als personenbezogene Daten anzusehen sind, weil mit Hilfe weiterer Informationen ein Personenbezug herstellbar ist. Dies entspricht auch der Position der Artikel-29-Gruppe der europäischen Datenschutzbehörden. In ihrem Positionspapier vom 20. Juni 2007 (WP 136 – http://ec.europa.eu) stellte sie fest, dass IP-Adressen – unabhängig davon, ob sie beim Zugangsvermittler oder beim Internet-Anbieter anfallen – als personenbezogen anzusehen sind, da sie sich auf eine bestimmbare Person beziehen.

In der Vergangenheit habe ich die Speicherung von IP-Adressen von Website-Nutzern durch Bundesbehörden bereits für unzulässig erklärt (vgl. etwa 22. TB Nr. 7.9) und eine entsprechende Änderung der Speicherungspraxis angemahnt. Leider beruft sich eine nicht geringe Anzahl der Bundesbehörden auf die Position des BMI: Das BMI will das Ergebnis eines Gerichtsverfahrens abwarten, in dem es um die Klage eines Bürgers gegen die Bundesregierung, vertreten durch das BMI, wegen der unzulässigen Speicherung von IP-Adressen beim Besuch von Internet-Angeboten der Bundesbehörden geht.

Ungeklärt ist nach Auffassung des BSI solange auch noch die Frage, in welcher Form die Nutzungsdaten auf Basis des BSI-Gesetzes verarbeitet werden dürfen. Das Gesetz trifft keine Festlegung dazu, ob IP-Adressen als personenbezogen anzusehen sind oder nicht. Eine Regelung gibt es jedoch für beide Fälle: die Protokolldaten, die im Kommunikationsnetz des Bundes anfallen, müssen – nur dann – vor der Verarbeitung zu Datensicherheitszwecken durch das BSI pseudonymisiert werden, wenn sie personenbezogene Daten enthalten (vgl. u. Nr. 5.2).

## 4.4 Ende eines langen Weges: Die EU-Telekommunikationsrichtlinien wurden beschlossen

*Mit ihrer Veröffentlichung im Amtsblatt der EU am 18. Dezember 2009 (L 337/11) sind die Änderungsrichtlinien zur Regulierung des Telekommunikationssektors in Kraft getreten und müssen bis zum 25. Mai 2011 in nationales Recht umgesetzt werden.*

Im Dezember 2009 war es endlich so weit. Die geänderten Richtlinien zur Regulierung des Telekommunikationssektors traten in Kraft. Mehr als zwei Jahre hatte die Revision gedauert, die die bestehenden Regelungen den Entwicklungen des Marktes anpassen und Bürgerinteressen stärker berücksichtigen sollte. Nach zähen Verhandlungen zu einigen strittigen Punkten (vgl. 22. TB Nr. 7.12) stimmte das EU-Parlament dem Reform-Paket zu.

Einige Änderungen betreffen die Datenschutzrichtlinie für elektronische Kommunikation, die sogenannte ePrivacy-Richtlinie. Bedeutsam ist die neu eingeführte Verpflichtung der Diensteanbieter, bei Datenschutzverletzungen die Betroffenen zu benachrichtigen – allerdings nur dann, wenn sie in ihrer Privatsphäre beeinträchtigt werden. Die zuständige Aufsichtsbehörde muss jedoch in allen Fällen benachrichtigt werden. Diese Verpflichtung leistet einen wesentlichen Beitrag zu mehr Transparenz für die Bürgerinnen und Bürger und gibt ihnen die Möglichkeit, im Falle einer Datenschutzverletzung auch selbst geeignete Gegenmaßnahmen zu ergreifen. Mit dieser Regelung wurde erstmalig eine verbindliche Verpflichtung zur Offenlegung von Datenschutzverstößen eingeführt. Es ist zu hoffen, dass eine entsprechende Vorgabe bei der Revision des EU-Rechtsrahmens für den Datenschutz allgemein eingeführt wird. Das allgemeine deutsche Datenschutzrecht sieht eine solche Regelung für nicht-öffentliche Stellen schon seit der BDSG-Novelle von September 2009 vor (vgl. o. Nr. 2.2).

Unerwünschte E-Mails waren schon in der „alten“ ePrivacy-Richtlinie verboten, die „neue“ Richtlinie erweitert und präzisiert das Verbot auf Werbe-E-Mails, die in betrügerischer Absicht gegen bestimmte Informationspflichten (z. B. klar erkennbare, unzweideutige und leicht zugängliche Bedingungen für die Inanspruchnahme eines Dienstes) verstoßen oder auf solche Websites verlinken, und will dadurch den zunehmenden Betrugsfällen im Internet Rechnung tragen. An der Wirksamkeit dieser Regelung habe ich jedoch meine Zweifel, denn Betrüger werden sich auch daran nicht halten.

Schon im Revisionsprozess gab eine weitere Regelung Anlass zu Diskussionen. Sie schreibt nämlich für Cookies, mit deren Hilfe Nutzungsprofile erstellt werden können („Tracking Cookies“), die informierte Einwilligung des Nutzers vor. Was für die Nutzer ein großer Schritt in Richtung Transparenz und Selbstbestimmung ist, wird von Diensteanbietern und den Werbenetzwerken als Hindernis bei ihren Geschäften angesehen. In letzter Minute und von vielen unbemerkt wurde daher in dem entsprechenden Erwägungsgrund der Hinweis aufgenommen, dass die Einwilligung auch durch die Einstellung des Browsers ausgesprochen werden kann – unter der Bedingung, dass „dies

technisch möglich und wirksam“ ist und die Einwilligung „ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage“ erfolgen kann.

Die derzeit verfügbaren Browser bieten jedoch nur sehr grob gestufte Optionen an. Hinzu kommt, dass die Standard-Einstellung in fast allen Fällen „Cookies akzeptieren“ vorgibt. Eine Information fehlt fast immer völlig. Dass diese Browser – jedenfalls bisher – wenig geeignet sind, eine wirksame informierte Einwilligung zu gewährleisten, ist nicht zu übersehen. Auch wenn sie gerne alles beim Alten ließen, sind jetzt die Website- und Werbeanbieter gefragt, die – möglicherweise zusammen mit den Browser-Herstellern – Lösungen erarbeiten müssen.

Ebenso positioniert sich auch die Artikel-29-Gruppe in ihrer Stellungnahme 2/2010 vom 22. Juni 2010 zu gezielter Werbung auf Basis der Auswertung des Surfverhaltens („Behavioural Targeting“): Sie fordert die informierte Einwilligung und sieht die Werbenetzwerke in der Pflicht, Opt-In-Mechanismen zu schaffen.

Die Diskussionen rund um den „Cookie-Paragraphen“ setzen sich hierzulande auch bei der Umsetzung der Richtlinie fort, an der derzeit gearbeitet wird. Denn die Änderung der Richtlinie macht auch eine entsprechende Anpassung des Telemediengesetzes (TMG) erforderlich. Das zuständige Bundeswirtschaftsministerium lehnt dies allerdings ab. Nach seiner Ansicht sei schon nach geltendem Recht eine Einwilligung für das Setzen von Cookies erforderlich – eine Position, die weder durch den Wortlaut noch durch die Begründung des TMG gestützt wird. Sie widerspricht auch der langjährigen aufsichtsbehördlichen Praxis und dem allgemein anerkannten Verständnis.

Der Düsseldorfer Kreis der Datenschutzaufsichtsbehörden hat in seinem Beschluss vom 25. November 2010 gefordert, das TMG entsprechend anzupassen, und unterstützt damit meine Position (vgl. Kasten zu Nr. 4.4). Vielleicht wird ja die BMI-Gesetzesinitiative zum Datenschutz im Internet, die „rote Linie“ (vgl. o. Nr. 4.1.3), im Gesetzgebungsverfahren so modifiziert, dass eine klare Einwilligungsregelung für Cookies geschaffen wird. Denn Cookies werden fast immer dann auf dem PC des Nutzers abgelegt, wenn – oftmals hinter seinem Rücken – ein Profil seiner Vorlieben und Interessen erstellt werden soll. Eine solche Praxis liegt nach meiner Auffassung jenseits des akzeptablen Bereichs und müsste durch eine „Rote Linie“ unterbunden werden.

Kasten zu Nr. 4.4

**Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich**
(Düsseldorfer Kreis am 24./25. November 2010)

**Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste**

Gegenwärtig wird über die Umsetzung der überarbeiteten Datenschutzrichtlinie für elektronische Kommunikationsdienste („ePrivacy Directive“) in nationales Recht beraten, die bis zum 24. Mai 2011 abgeschlossen sein muss. Die Richtlinie enthält in ihrem Artikel 5 Absatz 3 eine Regelung, die die datenschutzrechtlichen Voraussetzungen auch beim Umgang mit „cookies“ neu festlegt: Die bisherige Opt-Out-Lösung wird durch eine Opt-In-Lösung mit einer vorherigen umfassenden Information über die Zwecke der Verarbeitung ersetzt. Durch die Änderung der Richtlinie wird nun eine Anpassung des Telemediengesetzes hin zu einer informierten Einwilligung erforderlich, da im geltenden Telemediengesetz eine Widerspruchslösung umgesetzt ist (§ 15 Absatz 3 TMG).

Eine solche Änderung stößt auf erhebliche Widerstände auf Seiten des zuständigen Ministeriums, das eine Einwilligungslösung schon durch die in § 12 Absatz 1 und 2 TMG definierten allgemeinen Grundsätze realisiert sieht. Würde man dieser Auslegung folgen, müsste eine „alte“ Vorschrift zukünftig in „neuer“, zudem auch strengerer Weise ausgelegt und angewendet werden. Dies wäre nur schwer vermittelbar und möglicherweise kaum durchsetzbar.

Die Datenschutz-Aufsichtsbehörden betrachten bei ihrer Kontroll- und Aufsichtstätigkeit im Bereich der Telemedien § 15 Absatz 3 TMG als einschlägig für die Verwendung von „cookies“ in diesem Zusammenhang. Demnach sind Nutzungsprofile nur unter Verwendung eines Pseudonyms und vorbehaltlich eines Widerspruchs des Betroffenen zulässig. Nutzungsprofile werden in der Regel mit Hilfe von „cookies“ erstellt, die im „cookie“ gespeicherte eindeutige Identifikationsnummer (cookie-ID) wird entsprechend als Pseudonym angesehen. Diese Auslegung hat sich in der Praxis bewährt und wird allgemein anerkannt.

Die Umsetzung der „ePrivacy Directive“ erfordert daher eine gesetzliche Anpassung des TMG.

## 4.5 Gut aufgehoben? In den Fängen sozialer Netzwerke

*Immer mehr Menschen sind Mitglied sozialer Netzwerke. Umso wichtiger ist es, dass sie sorgsam mit ihren Daten umgehen. Aber auch die Betreiber müssen den Datenschutz und die Persönlichkeitsrechte der Nutzer wahren.*

Man muss nicht der „Generation Internet“ angehören – bei sozialen Netzwerken kann jeder mitmachen und immer mehr tun es auch, teils aus Neugier, teils um mitreden zu können. Oder weil Kollegen, Mitschüler und Freunde auch dabei sind.

Im Berichtszeitraum haben soziale Netzwerke immer wieder von sich reden gemacht, in den meisten Fällen nicht im positiven Sinne. Mit immer neuen „Ideen“, die vor der Privatsphäre nicht haltmachen, verärgern sie regelmäßig Mitglieder und vergraulen damit auch einige, die es eigentlich mal werden wollten.

So wurden bei verschiedenen sozialen Netzwerken AGB und Datenschutzbestimmungen geändert und den Mitgliedern eine Frist zur Einwilligung gesetzt, ansonsten drohte der „Rausschmiss“. Oder die E-Mail-Adressen aus

den hochgeladenen Adressbüchern von Mitgliedern wurden dafür genutzt, andere Mitglieder zu finden, die ebenfalls Kontakt zu den Adressen-Inhabern – oftmals Nichtmitglieder – hatten: So gerieten auch die ins Netz, die gar nicht vernetzt werden wollten. Profildaten wurden für Werbezwecke des Betreibers und Dritter verwendet – ungefragt, denn sie waren ja schon gespeichert. Zuletzt sorgte der „Gefällt-mir"-Button eines großen amerikanischen Netzwerks für Aufruhr. Mit diesem kleinen Knopf, der auf vielen Internet-Seiten zu finden ist, sammelt der Betreiber auch Informationen darüber, was seine Mitglieder außerhalb des Netzwerks machen und „mögen". Und die Mitglieder können sehen, was ihre „Freunde" mögen – eine einfache Werbestrategie.

Eine Reaktion der nationalen und internationalen Datenschutzbehörden konnte angesichts des forschen Umgangs mit personenbezogenen Daten durch die Netzwerkbetreiber nicht ausbleiben. Nach dem Düsseldorfer Kreis und der Internationalen Arbeitsgruppe für Datenschutz in der Telekommunikation hat die Artikel-29-Gruppe im Juni 2009 eine ausführliche „Stellungnahme zur Nutzung sozialer Online-Netzwerke" veröffentlicht, die auch im Internet abrufbar ist (WP 163 – http://ec.europa.eu). Sie richtet sich hauptsächlich an die Betreiber von Netzwerken, enthält aber auch hilfreiche Hinweise für die Nutzer.

Hier und da wurde zwischenzeitlich nachgebessert – Datenschutzerklärungen wurden überarbeitet und klarer strukturiert und Widerspruchsmöglichkeiten eingebaut. Mein Appell an die Nutzer ist weiterhin gültig: Gehen Sie sorgsam mit Ihren Daten um.

### 4.6 Und nun? Was wird aus dem Zugangserschwerungsgesetz?

*Am 23. Februar 2010 trat das Zugangserschwerungsgesetz (BGBl. I S. 78) in Kraft. Die dort festgelegten Netzsperren werden jedoch nicht umgesetzt. Es mehren sich Stimmen, die eine Rücknahme des Gesetzes fordern.*

Schon mit Bekanntwerden der Initiative zur Bekämpfung der Kinderpornografie Anfang 2009, die zuvor vom BKA-Präsidenten und der damaligen Bundesfamilienministerin angestoßen worden war, polarisierten die geplanten Netzsperren die Öffentlichkeit, Kinderschützer und Opfer ebenso wie Rechtsexperten und Bürgerrechtler. Anfänglich auf Basis einer Vereinbarung mit dem BKA sollten die Internet-Zugangsprovider anhand einer Liste des BKA den gesamten Internet-Verkehr filtern und Aufrufe einer Internet-Seite mit kinderpornografischen Inhalten mit einem Stopp-Schild beantworten. Die BKA-Liste sollte täglich aktualisiert und den Providern auf einem gesicherten Weg übermittelt werden.

Das folgende sehr kurze Gesetzgebungsverfahren wurde von teils lauten und emotionalen Diskussionen begleitet. Dass Kinderpornografie bekämpft werden muss, stand und steht außer Frage. Vielmehr ging es zum einen darum, ob Netzsperren überhaupt ein wirksames Mittel sind, wenn sie nachgewiesenermaßen mit geringem Aufwand und Sachverstand umgangen werden können. Zudem zweckentfremden Anbieter und Nutzer kinderpornographischen Materials immer wieder „normale" Techniken des Internets – wie z. B. das sog. Fast-Flux-Verfahren (vgl. Kasten zu Nr. 4.6) –, um elektronische Spuren zu verwischen. Damit wäre die Aktualität der BKA-Liste zumindest in Frage gestellt. Zum anderen wurde befürchtet, dass mit der Einrichtung der notwendigen technischen Infrastruktur der Weg für das Sperren und Filtern weiterer „unerwünschter" Inhalte durch staatliche Zensur eröffnet würde. Und dass sich eine solche Infrastruktur auch für wirtschaftliche Interessen einsetzen lässt, liegt auf der Hand.

Ich hielt es für problematisch, dass mit dem Abgleich mit der BKA-Liste ein Eingriff in das Fernmeldegeheimnis verbunden ist, ohne dass es hierfür eine gesetzliche Befugnis gab. Denn die technische Umsetzung der Netzsperren bedeutet eine Erweiterung des eigentlichen Zwecks der DNS-Abfragen (vgl. Kasten zu Nr. 6.4): Der technisch erforderlichen wurde eine zusätzliche Verarbeitung von Verkehrsdaten aller Internet-Nutzer hinzugefügt. Um zu entscheiden, ob anstelle der aufgerufenen Internet-Seite das Stopp-Schild geliefert wird, muss der Provider bei jedem Aufruf einer Internet-Seite prüfen, ob die Adresse der Seite mit einem Eintrag in der BKA-Liste identisch ist. Im Vordergrund der Diskussionen stand allerdings nicht die Verhältnismäßigkeit der Maßnahme, sondern die Frage, in welcher Form die Provider in die Pflicht genommen werden konnten. Da ein Grundrecht nicht durch eine einfache vertragliche Vereinbarung eingeschränkt werden kann, wurde in aller Eile ein Gesetz entworfen, das die Einschränkung legalisieren sollte.

Kurz vor Ende der 16. Legislaturperiode passierte das Gesetz den Bundestag und wurde nach einer intensiven Prüfung am 17. Februar 2010 vom Bundespräsidenten ausgefertigt. Dem BfDI wurde durch das Gesetz die Aufgabe zugewiesen, eine bei meiner Dienststelle angesiedelte Expertenkommission zu ernennen, die die Zulässigkeit der Einträge auf der BKA-Liste überwachen sollte. Ich habe mich im Gesetzgebungsverfahren gegen diese Aufgabenzuweisung gewandt, weil sie meine Unabhängigkeit beeinträchtigen und zudem die Reputation als unabhängige Datenschutzkontrollstelle beschädigen würde. Die seinerzeitige Bundestagsmehrheit ist diesen Argumenten allerdings nicht gefolgt.

Dann wurde es erst einmal still um die Netzsperren. Denn zwischenzeitlich hatte die neue Regierung in ihrer Koalitionsvereinbarung festgeschrieben, das Gesetz nicht anzuwenden. Sang und klanglos wurde somit das BKA vom BMI per Erlass angewiesen, keine Listen der Internet-Adressen mit kinderpornografischen Inhalten zu erstellen, was faktisch einer Nichtanwendung gleichkam. Ich halte das Vorgehen, ein vom Parlament beschlossenes Gesetz per Regierungserlass nicht anzuwenden, für verfassungsrechtlich äußerst problematisch, obwohl ich das damit verfolgte Ziel durchaus teile.

Da nach der Aussetzung des Gesetzes durch das BKA keine Sperrlisten erstellt wurden, sah ich auch keine Notwendigkeit mehr, das zu ihrer Kontrolle vorgesehene Expertengremium zu berufen.

Anlässlich der Anträge der verschiedenen Fraktionen, das Zugangserschwerungsgesetz aufzuheben, wurde im November 2010 in einer öffentlichen Anhörung des Rechtsausschusses des Deutschen Bundestages noch einmal die Meinung von Experten zur Verfassungsmäßigkeit und Erforderlichkeit eines Gesetzes eingeholt, das die Kontrolle eines jeden Internet-Zugriffs vorschreibt. Wie das Parlament letztlich entscheiden wird, bleibt abzuwarten.

Kasten zu Nr. 4.6

**Fast Flux**

Beim Aufruf von z. B. www.bfdi.bund.de wird vom DNS-Server die IP-Adresse 77.87.228.65 an den anfragenden Rechner geliefert. Für diese Namensauflösung im Internet ist das Domain Name System (DNS) verantwortlich, das auch zulässt, dass einem Namen mehrere IP-Adressen zugeordnet werden. Dies hat zur Folge, dass der Aufruf einer Adresse alle zugewiesenen IP-Adressen zurückliefert. Diese Technik kann in „guten" Netzwerken zur Lastenverteilung genutzt werden.

Aber auch Bot-Netze, die aus mit Schadsoftware infizierten PC bestehen, nutzen die Technik, um den Standort der Server zu verschleiern, auf denen sich die illegalen Inhalte tatsächlich befinden. Im DNS sind dann für eine Internet-Adresse hunderte oder sogar tausende IP-Adressen von infizierten PC eingetragen, die allerdings in diesen Netzen in sehr kurzen Zeitabständen ausgewechselt werden. Sie werden nach einem bestimmten Verfahren – mal die eine, mal die andere – an die Rechner geliefert, die die Adresse aufrufen. Die Anfrage landet auf diese Weise erst einmal bei einem infizierten PC. Da die infizierten PC so manipuliert sind, dass sie als Wegweiser zu dem tatsächlichen Speicherort dienen, liefern sie dem anfragenden Rechner die korrekte IP-Adresse, mit der dann der illegale Inhalt abgerufen wird.

## 4.7 „ACTA" – doch keine Vorratsdatenspeicherung im privaten Bereich

*Eine internationale Verpflichtung von Anbietern von Telekommunikationsdienstleistungen zur Überwachung ihrer Nutzer und eine Providerhaftung für Rechtsverstöße der Kunden konnten verhindert werden.*

Das Anti-Counterfeiting Trade Agreement (ACTA) soll als völkerrechtliches Abkommen zwischen der Europäischen Union, ihren Mitgliedstaaten und weiteren Staaten, darunter Australien, Japan, Kanada, Mexiko, die Schweiz und die USA, den Schutz geistigen Eigentums und der Urheberrechte im Internet stärken. Es soll die bestehenden Abkommen der Welthandelsorganisation ergänzen und einen internationalen Standard für den Schutz und die Durchsetzung des Rechts am geistigen Eigentum festlegen. Die über drei Jahre dauernden Verhandlungen, bei denen die EU-Mitgliedstaaten durch die Europäische Kommission vertreten wurden, hatten zunächst im Geheimen stattgefunden. Erst nach Protesten von Bürgerrechtlern entschloss sich die Kommission im April 2010 zu einer umfassenden Dokumentation auf ihrer Internetseite. Nachdem Anfang Oktober 2010 bei der Abschlusskonferenz in Tokio in fast allen wesentlichen Punkten Einigkeit erzielt worden war, wurde mit Fassung vom 3. Dezember 2010 der abschließende Vertragtext vorgelegt.

Bei den Beratungen ging es unter anderem darum, die Anbieter von TK-Dienstleistungen darauf zu verpflichten, ihre Nutzer mit Blick auf Verstöße etwa gegen das Urheberrecht zu überwachen. Bei Verletzung dieser „Überwachungspflichten" war eine eigene Haftung der Provider für eventuelle Rechtsverstöße ihrer Kunden angedacht. Da eine solche Überwachung nur auf der Grundlage der Speicherung entsprechender Daten stattfinden kann, stand unter datenschutzrechtlichen Gesichtspunkten die anlasslose Speicherung von IP-Adressen und TK-Verkehrsdaten zur Disposition. Letztlich wurde eine entsprechende Regelung aber nicht in den Vertragstext aufgenommen.

Insgesamt bewerte ich das erzielte Verhandlungsergebnis als Erfolg für das Datenschutzrecht. „ACTA" soll in den nächsten Monaten von den einzelnen Verhandlungspartnern ratifiziert werden.

## 4.8 IP-Beauskunftung zur Bekämpfung von Urheberrechtsverletzungen

*Internet-Anbieter, die auf Grund richterlicher Anordnung Auskunft über Name und Anschrift einer Person erteilen, der zu einem bestimmten Zeitpunkt eine konkrete IP-Adresse zugeteilt war, verstoßen nicht gegen das Datenschutzrecht. Trotzdem wirft die Praxis von Urheberrechtsinhabern Fragen auf.*

Im Berichtszeitraum hat sich eine Vielzahl von Bürgerinnen und Bürgern nach Erhalt von Abmahnschreiben der Rechteinhaber an meine Dienststelle gewandt und ihren Unmut darüber zum Ausdruck gebracht, dass der zuständige Internet-Zugangsprovider ihren Namen und ihre Anschrift an den Rechteinhaber beauskunftet und sie darüber nicht informiert hatte.

Aus datenschutzrechtlicher Sicht ist die Mitteilung von Kundendaten durch Anbieter von Internet-Zugangsdiensten an Rechteinhaber auf Basis gerichtlicher Anordnungen nicht zu beanstanden. Die Beauskunftung erfolgt nur auf eine richterliche Anordnung nach § 101 Absatz 9 Urheberrechtsgesetz (UrhG). Ohne eine solche Anordnung darf ein Anbieter die Daten nicht an private Dritte herausgeben. Anhand der Eingaben zu diesem Thema habe ich festgestellt, dass der Öffentlichkeit nicht bekannt ist, dass nach geltender Rechtslage der Provider nicht verpflichtet ist, seine Kunden über die Beauskunftung zu informieren. Auch darf er den *Inhalt* der Beauskunftung nicht speichern, so dass eine solche Auskunft an den Kunden bei Nachfrage nicht möglich ist.

Die Erteilung der Auskunft erfolgt praktisch in zwei Schritten. Zunächst erlässt das Gericht eine Anordnung, die Daten vorerst nicht zu löschen, im Nachgang wird dann nach Prüfung des Vorliegens der Voraussetzungen des § 101 UrhG die Anordnung erlassen, eine entsprechende Auskunft an den Antragsteller zu erteilen. Sollten bereits zum Zeitpunkt der ersten Anordnung keine Daten mehr beim Anbieter vorhanden sein, erhält der Rechtein-

haber keine Auskunft. Das kann passieren, denn die Anbieter haben die Nutzungsdaten nach Beendigung der Inanspruchnahme unverzüglich zu löschen und dürfen deshalb auch die Zugangsdaten nur kurze Zeit (höchstens sieben Tage) aufbewahren, soweit dies für Abrechnungszwecke, zur Störungseingrenzung und zur Aufklärung von Missbrauchsfällen erforderlich ist.

Der Frage, ob der in Anspruch genommene Bürger tatsächlich widerrechtlich ein urheberrechtlich geschütztes Werk aus dem Internet heruntergeladen hat, kann meine Dienststelle nicht nachgehen. Hierfür steht der Zivilrechtsweg offen.

Unabhängig von der dargestellten Rechtslage stellt sich jedoch die Frage, ob die Praxis von spezialisierten Unternehmen und Kanzleien, massenweise IP-Adressen von Tauschbörsennutzern zu speichern und auszuwerten, mit den Grundsätzen der Datensparsamkeit und Transparenz vereinbar ist. Auch die formularmäßigen und bisweilen nicht spezifizierten Auskunftsersuchen verursachen einen schalen Beigeschmack.

Sehr kritisch stehe ich auch Forderungen gegenüber, auf Grund gesetzlicher Vorgaben zu Zwecken der Aufklärung schwerer Straftaten auf Vorrat gespeicherte Daten (vgl. Nr. 6.1) auch zur Bekämpfung von Urheberrechtsverstößen zu verwenden. Das Bundesverfassungsgericht hat derartigen Ansinnen glücklicherweise einen Riegel vorgeschoben.

## 4.9 Das Gemeinsame Internetzentrum der Sicherheitsbehörden

*Die Tätigkeit des Gemeinsamen Internetzentrum (GIZ) greift in das Recht der Betroffenen auf informationelle Selbstbestimmung ein.*

Beim GIZ handelt es sich um ein Kooperationsforum, in dem die beteiligten Behörden – Bundesamt für Verfassungsschutz, Bundeskriminalamt, Bundesnachrichtendienst, Militärischer Abschirmdienst und Generalbundesanwalt – ihre fachlichen, sprachlichen und technischen Kompetenzen bündeln, um im Internet nach Informationen zu suchen, die auf extremistische und terroristische Aktivitäten hinweisen.

Die beteiligten Behörden beobachten zu diesem Zweck insbesondere islamistische Websites, einschlägige Newsgroups, Foren und Chatrooms und werten deren Informationsgehalt aus. Die so gewonnenen Informationen werden in einem periodischen oder anlassbezogenen Bericht (dem sog. GIZ-LOG) zusammengefasst und den Kooperationspartnern zur Verfügung gestellt. In seiner Rede zur Vorstellung des GIZ im Oktober 2007 erklärte der damalige Bundesminister des Innern, dass das GIZ ausschließlich das offene, jedem zugängliche Internet überwache und somit eine Aufgabe wahrnehme, für die keine besonderen Hoheitsbefugnisse erforderlich seien.

Was auf den ersten Blick plausibel erscheint, stellt sich bei genauerer Betrachtung unstimmig dar. Ich bin im Dezember 2009 im Rahmen eines Beratungs- und Kontrollbesuchs im GIZ der Frage nachgegangen, ob durch die Aktivitäten dieses Forums in das Recht auf informationelle Selbstbestimmung von Betroffenen eingegriffen wird.

Das Bundesverfassungsgericht hat in seinem Urteil vom 27. Februar 2008 zur sog. Online-Durchsuchung (BVerfG 1 BvR 370/07 – vgl. auch 22. TB Nr. 4.1.1) festgestellt, die Kenntnisnahme öffentlich zugänglicher Informationen sei dem Staat grundsätzlich nicht verwehrt. Das gelte auch, wenn im Einzelfall personenbezogene Informationen erhoben werden können, beispielsweise bei der Teilnahme an Chats und Diskussionsforen unter Pseudonym, solange die Behörde hierbei kein schutzwürdiges Vertrauen des Betroffenen in die Identität und Motivation seines Kommunikationspartners ausnutze. Dies bedeutet: Wenn sich eine Sicherheitsbehörde in Chats oder Foren bewegt, in denen es ausreicht, einen fiktiven Namen und ein Passwort zur Anmeldung zu wählen, um teilzunehmen, ist das schutzwürdige Interesse des Betroffenen nicht berührt.

Wenn ein Hoheitsträger im Rahmen der Anmeldung zu einem Chat oder einem Diskussionsforum fingierte, detaillierte personenbezogene Angaben z. B. zu Name, Adresse, Telefonnummer, E-Mail-Adresse etc. macht, die seine Zugehörigkeit zu einer Behörde verschleiern, wird schutzwürdiges Vertrauen in Anspruch genommen. Meines Erachtens wird auch durch die aktive Teilnahme an Chats und Foren das schutzwürdige Interesse des Kommunikationspartners ausgenutzt. Da es in verschiedenen Kommunikationsplattformen erforderlich ist, die Mitgliedschaft durch eigene Beiträge aktiv zu halten, müsste eine Behörde zur Aufrechterhaltung des Zugangs eigene Beiträge einstellen. Damit könnte sie, wenn sie etwa Fragen eines anderen Forumsteilnehmers beantwortet, den Eindruck einer aktiven Unterstützung der Gemeinschaft erwecken.

Zwar mag es im Einzelfall schwer sein festzustellen, ab welchem Stadium der Internet-Recherche durch eine Behörde das schutzwürdige Vertrauen des Betroffenen in die Integrität des Kommunikationspartners ausgenutzt wird. Nach der o. g. verfassungsgerichtlichen Rechtssprechung ist aber jedenfalls immer dann von einem Eingriff in das informationelle Selbstbestimmungsrecht auszugehen, wenn die dabei erhobenen Daten gezielt zusammentragen, gespeichert und unter Hinzuziehung weiterer Daten ausgewertet werden. Gerade dies ist Aufgabe und Ziel des GIZ. Die Tätigkeit der an ihm beteiligten Sicherheitsbehörden bedarf daher einer Rechtsgrundlage (vgl. a. Nr. 7.1.7).

## 4.10 Veröffentlichung von Wahlvorschlägen im Internet

*Die Veröffentlichung von Wahlbewerbern im Internet bedarf einer ausdrücklichen Rechtsgrundlage.*

Ein Petent, der als Kandidat an der Europawahl 2009 teilgenommen hatte, beschwerte sich darüber, dass der Bundeswahlleiter auf seiner Internetseite personenbezogene Angaben zu den Kandidaten ohne eine Rechtsgrundlage oder eine entsprechende Einwilligung veröffentlicht habe.

Nach Prüfung bin ich zu der Bewertung gekommen, dass für derartige Internetveröffentlichungen eine ausdrückli-

che Rechtsgrundlage erforderlich wäre, eine solche aber nicht existiert. Die Veröffentlichung von Wahlvorschlägen zur Europawahl richtet sich ausschließlich nach Artikel 79 Absatz 1 Europawahlordnung. Danach hat die vorgeschriebene öffentliche Bekanntmachung durch den Bundeswahlleiter im Bundesanzeiger zu erfolgen. Alternativen oder zusätzliche Formen der Veröffentlichung sieht die Europawahlordnung nicht vor. Für eine Veröffentlichung im Internet ist eine ausdrückliche Rechtsgrundlage erforderlich, da mit der Einstellung der personenbezogenen Angaben in das Internet – insbesondere aufgrund der erheblich leichteren Recherchemöglichkeiten – ein qualitativ anderer Eingriff in das Recht auf informationelle Selbstbestimmung verbunden ist, als mit der vorgegebenen öffentlichen Bekanntmachung im Bundesanzeiger. Ich habe den Bundeswahlleiter daher gebeten, künftig die Veröffentlichung ausschließlich nach dem gesetzlich normierten Verfahren vorzunehmen.

Gleichwohl halte ich es durchaus für sinnvoll, auch das Internet als Informationsmedium für die Wählerinnen und Wähler zu nutzen. Es sollte daher eine ausdrückliche Rechtsgrundlage für die Veröffentlichung von Wahlbewerbern im Internet geschaffen werden. Um eine datenschutzgerechte Ausgestaltung der Internetveröffentlichungen zu gewährleisten, sollten zusätzlich Regelungen getroffen werden, die sicherstellen, dass die Veröffentlichungen unversehrt, vollständig und aktuell bleiben und jederzeit ihrem Ursprung nach zugeordnet werden können. Weiter sollten technische Vorgaben zur Veröffentlichung im Internet festgelegt werden, die es erschweren, die Daten automatisiert zu erschließen und mit anderen Daten abzugleichen. So könnte etwa vorgegeben werden, die Daten der Wahlbewerber nur als Bilddatei einzustellen, wodurch sie für Suchmaschinen in der Regel nicht auswertbar wären. Ferner sollten immer nur einzelne (wenige) Daten zu jeweils einem Bewerber pro Seite abrufbar sein. Auch sollte die Möglichkeit zum Download dieser Daten erschwert werden. Wünschenswert wäre insbesondere, dass es keine Liste(n) mit allen Bewerbern und allen personenbezogenen Daten gibt.

Mit dem Bundeswahlleiter habe ich grundsätzliches Einvernehmen erzielt. Er hat darüber hinaus noch weitergehende oder alternative Vorschläge gemacht, die ich sehr begrüße.

Ich empfehle daher, eine entsprechende Gesetzesänderung in die Wege zu leiten. Eine solche Regelung, die der besonderen Qualität von Internetveröffentlichungen durch entsprechende Gestaltungsvorgaben Rechnung trägt, könnte vorbildhaft auch für andere Bereiche sein, in denen die Veröffentlichung personenbezogener Daten im Internet erfolgen soll.

### 4.11 Verbesserte internationale Datenschutzkooperation

*Angesichts zunehmend globaler Datenströme wird eine engere Zusammenarbeit der nationalen Datenschutzbehörden immer wichtiger. Zur Verbesserung der internationalen Kooperation wurden verschiedene Initiativen ergriffen, an denen auch ich mich aktiv beteiligt habe.*

Im April 2010 haben zehn nationale Datenschutzbehörden in einem gemeinsamen Brief Google aufgefordert, die Privatsphäre seiner Nutzer beim neuen Dienst „Google Buzz“ besser zu schützen[1]. Durch die Markteinführung von „Google Buzz“ wurde der bisherige Google-Mail-Dienst („Gmail“) zu einem sozialen Netzwerkdienst ausgebaut. Die Datenschutzbehörden kritisieren in ihrem Schreiben insbesondere, dass personenbezogene Daten der Nutzer offengelegt wurden, ohne dass diese vorher angemessen informiert wurden und somit nicht in der Lage waren, selbst über die Nutzung ihrer Daten zu entscheiden. Das Unternehmen hat die bei der Einführung von „Buzz“ erfolgten Datenschutzverstöße öffentlich bedauert.

Ebenfalls im Frühjahr 2010 wurde das „Global Privacy Enforcement Network“ (GPEN) als informeller Zusammenschluss nationaler Datenschutzbehörden errichtet. Ziel des Netzwerkes ist es, die internationale Zusammenarbeit im Bereich der Durchsetzung des Datenschutzrechts zu verbessern. Vorgesehen sind u. a. ein regelmäßiger Erfahrungsaustausch zwischen den Mitgliedern sowie die Durchführung von Fortbildungsmaßnahmen gemeinsam mit Vertretern von Wirtschaft, Wissenschaft oder internationaler Organisationen. Auch sollen Maßnahmen bilateraler Unterstützung und Kooperation vereinbart werden. Verabredet wurden die Durchführung regelmäßiger Telefonkonferenzen sowie Treffen am Rande internationaler Sitzungen, wie etwa der Internationalen Datenschutzkonferenz. Darüber hinaus wurde zur Unterstützung der Arbeit des Netzwerkes durch die OECD eine Website eingerichtet, die neben einem öffentlichen auch über einen internen Bereich verfügt (siehe https://www.privacyenforcement.net/).

In den Jahren 2009 und 2010 fanden insgesamt vier „Case Handling Workshops“ statt, an denen Angehörige meiner Dienststelle teilgenommen haben. Diese Treffen wurden von der Europäischen Konferenz der Datenschutzbeauftragten ins Leben gerufen, um Erfahrungen und Kenntnisse auszutauschen und auf diesem Wege bei der Bearbeitung von Bürgereingaben und bei der Behandlung von ähnlich gelagerten Sachfragen zu einer vergleichbaren Verfahrensweise zu gelangen. Die Case Handling Workshops unterscheiden sich von anderen Foren der europäischen Zusammenarbeit dadurch, dass die Zielgruppe hier in erster Linie diejenigen Mitarbeiter der Datenschutzbehörden sind, die sich mit konkreten Problemen und Fragestellungen beschäftigen (Sachbearbeiter). Die letzten beiden Workshops wurden in Brüssel (März 2010) und in Manchester (September 2010) zu den Schwerpunkt-Themen Datenschutz in der Forschung und im Gesundheitswesen, Datenschutz bei modernen Mobilitätssystemen sowie effiziente Wege und Methoden der Bearbeitung von Fällen und Beschwerden organisiert. Die Case Handling Workshops stehen nicht nur Angehörigen der Datenschutzkontrollstellen aus Ländern der EU, sondern aus ganz Europa offen.

[1] Der gemeinsame Brief wurde von den Datenschutzbehörden von Kanada, Frankreich, Irland, Israel, Italien, Niederlande, Neuseeland, Spanien, Großbritannien und Deutschland unterzeichnet.

## 5 Technologischer Datenschutz

*Auch wenn Datenschutz traditionell als vorwiegend juristische Materie verstanden wird, nimmt die Bedeutung der Technik für die Bedrohung aber auch für den Schutz der Privatsphäre kontinuierlich zu.*

Datenschutz durch Technik – dieses Thema durchzieht die Tätigkeitsberichte der Datenschutzbeauftragten von Bund und Ländern seit vielen Jahren. Trotzdem handelt es sich dabei um alles andere als einen verstaubten Ladenhüter. Vielmehr scheint es sich inzwischen auch bei eher datenschutzfernen IT-Spezialisten und Anwendern herumgesprochen zu haben, dass neue Produkte, Dienste und Geschäftsmodelle nicht ohne entsprechende Schutzmechanismen auskommen. Wer diese Lehre noch nicht beherzigt hat, dem ist zu raten, sich einmal näher mit den Datenschutzskandalen und spektakulären Datenmissbrauchsfällen zu beschäftigen, gerade im Hinblick auf das Image der betroffenen Unternehmen, aber auch in Bezug auf das Schadenspotenzial.

Technologischer Datenschutz und geschäftlicher Erfolg – dies kann sogar eine Win-Win-Konstellation werden, jedenfalls dann, wenn der Vorsprung beim Datenschutz als Wettbewerbsinstrument eingesetzt wird. Auch aus diesem Grund setze ich mich seit langem für das Datenschutz-Audit ein, also für Prüfsiegel für solche Produkte, Dienste und Unternehmen, die einen besonders hohen Datenschutzstandard garantieren. Auch die Zertifizierung technischer Systeme anhand von Schutzprofilen (vgl. etwa 22. TB Nr. 8.1) fällt in diese Kategorie.

Datenschutz und IT-Sicherheit gehen Hand in Hand – jedenfalls meistens, wie etwa bei der Entwicklung neuer Sicherheitsstandards für die Mobilkommunikation (vgl. Nr. 5.11). Bisweilen kommt es jedoch auch zu Gegensätzen, etwa wenn mit dem Argument der Anhebung der IT-Sicherheit zusätzliche Überwachungsmöglichkeiten gefordert werden (vgl. Nr. 5.2).

Fragen des technologischen Datenschutzes ziehen sich durch alle Kapitel dieses Berichts. Er bildet ein Kernelement der Modernisierung des Datenschutzrechts (vgl. Nr. 1), spiegelt sich in Maßnahmen zur Weiterentwicklung des datenschutzrechtlichen Rahmens (vgl. Nr. 2.3 und 2.4) und hat in Planungen für eine „Stiftung Datenschutz“ Eingang gefunden (vgl. Nr. 2.5). Natürlich ist auch die „elektronische Identität“ (vgl. Nr. 3) ein Thema des technologischen Datenschutzes, vom Internet (Nr. 4) ganz zu schweigen. Ob Telekommunikations- und Postdienste (Nr. 6) oder Projekte zur Inneren Sicherheit (Nr. 7) – überall werden auch Fragen der Technik behandelt und selbst bei der Inneren Verwaltung und im Rechtswesen (Nr. 8), bei den Finanzen (Nr. 9), in den Bereichen Wirtschaft und Verkehr (Nr. 10), Gesundheit und Soziales (Nr. 11) und des Mitarbeiterdatenschutzes (Nr. 12) finden sich zahlreiche Projekte, bei denen technologisches Datenschutz-Know-How gefragt ist.

Technologischer Datenschutz wird von Menschen gemacht – deshalb freue ich mich darüber, dass ich das BfDI-Team im Berichtszeitraum um zusätzliche IT-Spezialistinnen und -Spezialisten erweitern konnte (vgl. Nr. 14.4). Damit hat sich die technische Beratungs- und Prüfkompetenz meiner Dienststelle signifikant verbessert.

Dass sich schließlich auch die Bundesregierung in ressortübergreifenden Projekten mit datenschutzrelevanten Themen beschäftigt, kann da nicht verwundern – auch wenn die Ergebnisse bisweilen zu wünschen übrig lassen.

Bereits zum fünften Mal fand im Jahre 2010 der Nationale IT-Gipfel statt – ein jährliches Treffen von hochrangigen Vertretern aus Politik, Wirtschaft und Wissenschaft. Leider werden dabei Fragen des Daten- und Verbraucherschutzes aber nur selten angemessen in den Blick genommen. Insbesondere hätte man vom 5. IT-Gipfel 2010 in Dresden mehr erwarten können. Im Vordergrund der Diskussionen dieses Jahres stand die neue IKT-Strategie „Deutschland Digital 2015“. Die Interessen der Bürgerinnen und Bürger hinsichtlich des Daten- und Verbraucherschutzes wurden jedoch kaum berücksichtigt. Im Vorfeld des IT-Gipfels habe ich daher zusammen mit dem Vorstand des Verbraucherzentrale Bundesverbandes (vzbv) einen Fünf-Punkte-Katalog veröffentlicht, damit bei digitalen Großprojekten Daten- und Verbraucherschutz nicht unter die Räder kommen (vgl. Kasten a zu Nr. 5)

Mit dem IT-Planungsrat wurde im Berichtszeitraum ein Gremium zur Koordinierung von IT-Themen zwischen Bund, Ländern und Kommunen geschaffen. Bereits im August 2009 wurde der entsprechende Artikel 91c in das Grundgesetz aufgenommen (vgl. Kasten b zu Nr. 5.). Als dessen beratendes Mitglied habe ich die Einbeziehung eines Vertreters der Landesbeauftragten für den Datenschutz unterstützt.

Auf seiner Sitzung am 24. September 2010 hat der IT-Planungsrat die Nationale E-Government-Strategie beschlossen. Nicht zuletzt durch meine Beteiligung an der Vorbereitung der Nationalen E-Government-Strategie wurden Datenschutz und Informationsfreiheit als eines der sechs zentralen Ziele definiert. So ist festgelegt, dass sich entsprechende Anwendungen an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten haben und Verwaltungsdienstleistungen soweit möglich auch anonym oder unter Pseudonym in Anspruch genommen werden können. Die angestrebte Bündelung von Aufgaben und die ebenenübergreifende Kooperation verschiedener Verwaltungsträger und Behörden kann nur unter strikter Beachtung der Persönlichkeitsrechte und des Prinzips der informationellen Gewaltenteilung durchgeführt werden.

Außerdem ist in der Nationalen E-Government-Strategie die Verpflichtung verankert, geeignete Informationen aus Politik und Verwaltung der Öffentlichkeit zur Verfügung zu stellen und damit die Idee des Open Government mit Leben zu erfüllen. Darüber freue ich mich insbesondere im Hinblick auf meine zweite Zuständigkeit, die Informationsfreiheit.

Kasten a zu Nr. 5

**Fünf-Punkte-Katalog**

1. Technologischen Datenschutz stärken

   Bei der Entwicklung neuer Technologien müssen die Erfordernisse des Datenschutzes frühzeitig berücksichtigt werden („privacy by design“). Zudem sollten die Voreinstellungen von Sozialen Netzwerken oder bei Browsern standardmäßig ein hohes Datenschutz- und Verbraucherschutzniveau aufweisen („privacy by default“).

2. Datenerhebung und -verarbeitung transparent gestalten

   Informationen über eingesetzten Techniken der Datenerhebung und -verarbeitung müssen situativ angemessen, verständlich und leicht abrufbar sein. Einwilligungen in die Erhebung und Verarbeitung von Daten sollten zeitlich begrenzt sein. Eine aktive, informierte Einwilligung ist verbindlich umzusetzen.

3. Gesetzlichen Rahmen verbessern

   Die wesentlichen Verbraucher- und Datenschutzrechte gehören ins Gesetz. Dazu gehört ein verbrieftes Widerspruchsrecht der Betroffenen gegen die Veröffentlichung ihrer Daten im Internet sowie das Verbot Profile nicht ohne Einwilligung des Betroffenen zu erstellen.

4. Freiwillige Selbstverpflichtungen verbindlicher machen

   Freiwillige Selbstverpflichtungen, wie der kürzlich präsentierte Datenschutz-Kodex von Anbietern von Geodaten-Diensten (zum Beispiel Google Street View), sind grundsätzlich zu begrüßen. Sie müssen aber mit Kontrollen und Sanktionen bei Nichteinhaltung begleitet werden. Eine Selbstverpflichtung ersetzt kein verbrieftes, einklagbares Recht auf Widerspruch.

5. Verbraucher- und Datenschutz international durchsetzen

   Das Surfen im Internet ist längst – obwohl vor Ort durchgeführt – eine globale Angelegenheit. Internetdienste, die unter das sogenannte Safe Harbor-Abkommen fallen, müssen sich an europäisches beziehungsweise nationales Recht halten und dies auch gegenüber den Nutzern kenntlich machen. Um dies zu erreichen, muss das Abkommen verbessert und effektiv durchgesetzt werden.

Kasten b zu Nr. 5

**Artikel 91c Grundgesetz**

(1) Bund und Länder können bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgabenerfüllung benötigten informationstechnischen Systeme zusammenwirken.

(2) Bund und Länder können auf Grund von Vereinbarungen die für die Kommunikation zwischen ihren informationstechnischen Systemen notwendigen Standards und Sicherheitsanforderungen festlegen. Vereinbarungen über die Grundlagen der Zusammenarbeit nach Satz 1 können für einzelne nach Inhalt und Ausmaß bestimmte Aufgaben vorsehen, dass nähere Regelungen bei Zustimmung einer in der Vereinbarung zu bestimmenden qualifizierten Mehrheit für Bund und Länder in Kraft treten. Sie bedürfen der Zustimmung des Bundestages und der Volksvertretungen der beteiligten Länder; das Recht zur Kündigung dieser Vereinbarungen kann nicht ausgeschlossen werden. Die Vereinbarungen regeln auch die Kostentragung.

(3) Die Länder können darüber hinaus den gemeinschaftlichen Betrieb informationstechnischer Systeme sowie die Errichtung von dazu bestimmten Einrichtungen vereinbaren.

(4) Der Bund errichtet zur Verbindung der informationstechnischen Netze des Bundes und der Länder ein Verbindungsnetz. Das Nähere zur Errichtung und zum Betrieb des Verbindungsnetzes regelt ein Bundesgesetz mit Zustimmung des Bundesrates.

## 5.1 Smart Metering – Der intelligente Stromzähler

*Die Sicherung einer nachhaltigen Energieversorgung ist ein wichtiges Ziel, das auch eine sparsame und umweltfreundliche Produktion sowie Verteilung umfasst – allerdings nicht zum Preis eines gläsernen Energieverbrauchers.*

Der Anspruch der Nachhaltigkeit bedingt den breitflächigen Einsatz erneuerbarer Energien sowie eine Erhöhung der Energieeffizienz. Die Energieerzeugung aus erneuerbaren Energien stellt die Versorgungsunternehmen dabei vor neue Herausforderungen und bedarf intelligenter Verknüpfungen von Energieerzeugung, Transport, Speicherung und Verbrauch. Mit Hilfe intelligenter Stromnetze sowie dem Einsatz neuer Mess- und Steuerungstechnik soll

sichergestellt werden, dass die richtige Energiemenge „just in time“ produziert und ohne teure Zwischen- und Vorhaltespeicherung zur Verfügung gestellt werden kann. Hierzu sind mehr Verbrauchs- und Steuerungsinformationen notwendig, als die konventionelle analoge Mess- und Regelungstechnik anbieten kann.

Ein erster Schritt auf dem Weg zu einer effizienteren Energieerzeugung und -nutzung ist das Angebot von Tarifen, mit denen Anreize für eine individuelle Steuerung des Energieverbrauches und damit zur Energieeinsparung gegeben werden. Um den tatsächlichen Verbrauch sowie die tatsächliche Nutzungszeit anzuzeigen und damit einen effektiveren Einsatz von Ressourcen zu ermöglichen, ist gemäß einer EG-Richtlinie (2006/32/EG) der Einbau neuer intelligenter Stromzähler, so genannter Smart Meters, in allen EU-Mitgliedstaaten verpflichtend. Dementsprechend sind derartige Zähler nach § 21b Absatz 3a Energiewirtschaftsgesetz seit dem 1. Januar 2010 grundsätzlich in Neubauten und bei größeren Renovierungsmaßnahmen einzubauen, damit die spätestens ab dem Jahreswechsel 2010/2011 von den Energieversorgern anzubietenden Spartarife von den Verbrauchern auch tatsächlich genutzt werden können.

Viele unserer Aktivitäten in Beruf, Familie und Freizeit sind technikgestützt und spiegeln sich gerätebezogen in einem nach Energieeinsatz und Nutzungszeit spezifischen Verbrauchsprofil wider. Aus diesem „Datenschatten“ wird mit einer gerätebezogenen Verbrauchsmessung eine immer präzisere Abbildung der individuellen und höchst persönlichen Aktivitäten möglich. Punktuell und in Echtzeit wird die einzelne Aktivität erkennbar. Über den Tag ergibt sich auf diesem Weg ein Ablaufprotokoll, das wesentliche Informationen für ein Verhaltensprofil enthält. Damit wird deutlich, dass ein datenschutzkonformes Konzept für die neuen Mess- und Energiespartechniken unverzichtbar ist, wenn der gläserne Energieverbraucher vermieden werden soll.

„Privacy by Design“ ist der Schlüsselbegriff für solche datenschutzfreundliche Lösungen. Er bedeutet zunächst, die Auswirkungen künftiger neuer Informationstechnologien frühzeitig zu erkennen und zu hinterfragen. Privacy by Design erfordert aber auch, der Erkenntnis Taten folgen zu lassen und Risiken und Missbrauchsgefahren nicht nur juristisch durch Verbote und Sanktionsnormen, sondern so früh wie möglich auch bei der Verfahrens- und Produktentwicklung durch ein datenschutzkonformes technisches Design zu reduzieren (vgl. auch Nr. 3.1).

Für die datenschutzgerechte Konzeption von Smart Metering bedeutet dies eine Erforderlichkeitsprüfung für jede geplante Erhebung, Speicherung und Nutzung personenbezogener Daten, frühestmögliche Anonymisierung oder Pseudonymisierung auf der untersten Systemstufe sowie volle Transparenz und uneingeschränkte Datenautonomie für den Verbraucher. Diesem darf keine „Black Box“ aufgedrängt werden, deren Speicherungs-, Auswertungs-, Übermittlungs- und Fernsteuerungsfunktionen für ihn nicht durchschaubar sind. Die Betroffenen müssen die Datenhoheit über ihre Verbrauchsdaten behalten.

Die Konferenz der Datenschutzbeauftragten von Bund und Ländern hat bei der digitalen Messung und Steuerung des Energieverbrauches ein datenschutzrechtliches Regelungsdefizit festgestellt (vgl. Kasten zu Nr. 5.1). Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen schützen die Privatsphäre der Verbraucher nur unzureichend. Die Datenschutzkonferenz fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der digital erhobenen Verbrauchsinformationen.

Ich habe mich im parlamentarischen Raum sowie beim BMWi für eine datenschutzfreundliche und sichere Informationsverarbeitung beim Smart Metering eingesetzt. Auf meine Anregung hin haben das Ministerium und das Bundesamt für Sicherheit in der Informationstechnik die Arbeit an sicheren Schutzprofilen für die neue Mess- und Steuerungstechnologie aufgenommen. Eine Novellierung des Energiewirtschaftsgesetzes, die auch Regelungen zum Smart Metering enthalten wird, steht unmittelbar bevor. Im Rahmen dieses Gesetzgebungsverfahrens werde ich auf eine datenschutzgerechte Ausgestaltung der Bestimmungen dringen.

Kasten zu Nr. 5.1

**Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010**

**Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs**

Das Energiewirtschaftsgesetz legt fest, dass seit Anfang des Jahres 2010 digitale Zähler in Häuser und Wohnungen eingebaut werden müssen, die den tatsächlichen Energieverbrauch (z. B. Strom und Gas) und die tatsächliche Nutzungszeit messen (Smart Metering). Damit sollen Verbraucher ihren Energieverbrauch künftig besser kontrollieren und steuern können und zur Verbesserung der Energieeffizienz beitragen.

Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können. Viele Handlungen des täglichen Lebens in der Wohnung führen zumindest mittelbar zum Verbrauch von Energie. In der Nutzung dieser Ressourcen spiegeln sich somit Tagesabläufe wider. Die detaillierte Erfassung des Verbrauchs birgt daher ein hohes Ausforschungspotenzial bezüglich der Lebensgewohnheiten der Betroffenen in sich. Dies gilt in besonderem Maße, wenn neben neben

dem Gesamtverbrauch im häuslichen Bereich auch der Verbrauch einzelner Endgeräte erfasst wird. Zusätzliche Risiken entstehen, wenn die digitalen Zähler zu Steuerungszentralen für im Haushalt betriebene Geräte ausgebaut werden.

Die detaillierte Erfassung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten.

Eine effiziente Energiedistribution und -nutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen. Eine solche Regelung muss die schutzwürdigen Interessen der Betroffenen berücksichtigen und eine strikte Zweckbindung der erhobenen personenbezogenen Daten vorschreiben. Die Regelung muss zudem sicherstellen, dass die Prinzipien der Transparenz der Datenverarbeitung beachtet und die Betroffenenrechte gewahrt werden.

Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen. Dies gilt insbesondere für den Grundsatz der Datenvermeidung und für die Datensouveränität der Betroffenen. So ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Für digitale Zähler und intelligente Verteil- bzw. Verarbeitungsnetze (Smart Grids) sind technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Hierzu gehört auch die Verschlüsselung personenbezogener Verbrauchsdaten. Die Anforderungen an den technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen. Für die Datenverarbeitungssysteme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.

## 5.2 Neues BSI-Gesetz

*Bei der gesetzlichen Neuregelung zur Regelung der Befugnisse für das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurden meine Anregungen im wesentlichen aufgegriffen.*

Bereits seit längerem verfolgt das BMI das Ziel, das BSI zu einer mit Eingriffsbefugnissen ausgestatteten Sicherheitsbehörde auszubauen. Das BSI ist ursprünglich aus der – nachrichtendienstlich orientierten – Zentralstelle für das Chiffrierwesen entstanden. Heute bildet die technische Unterstützung der Nachrichtendienste und Ermittlungsbehörden allerdings nur noch einen Teilbereich des BSI-Aufgabenspektrums. Zu seinen Aufgaben gehören verschiedene Initiativen zur Stärkung der IT-Sicherheit, darunter auch Serviceleistungen für die Öffentlichkeit. Außerdem wurde es gesetzlich bereits vor Jahren zur Hilfestellung gegenüber dem BfDI in Fragen des technologischen Datenschutzes verpflichtet.

In Weiterentwicklung der bereits vom BSI wahrgenommenen Aufgaben zum Schutz der IT-Infrastrukturen des Bundes strebte die Bundesregierung in der 16. Legislaturperiode an, das Amt mit direkten Eingriffsbefugnissen in die Kommunikationsbeziehungen zwischen Bundesbehörden und externen Dritten auszustatten. Der Regierungsentwurf vom 8. Juli 2008 enthielt dazu folgende Regelungen:

- Das Bundesamt erhält die Befugnis
  1. Protokolldaten einschließlich Telekommunikationsverbindungsdaten, die beim Betrieb von Informationstechnik des Bundes anfallen, zu erheben, zu verarbeiten und zu nutzen, und
  2. Telekommunikationsinhalte, die beim Betrieb von Informationstechnik des Bundes anfallen, zum Zweck der Entdeckung von Schadprogrammen auszuwerten.
- Das Bundesamt kann gegenüber den Betreibern im Einzelfall konkrete Vorgaben für die technische Sicherung der Kommunikationstechnik des Bundes oder von Teilen machen.
- Zur Abwehr einer im einzelnen Fall bestehenden gegenwärtigen Gefahr für die Kommunikationstechnik des Bundes kann das Bundesamt die notwendigen Maßnahmen gegenüber den Betreibern der Kommunikationstechnik des Bundes oder Teilen anordnen, insbesondere die Abschaltung von bestimmten informationstechnischen Einrichtungen, die Installation zusätzlicher Informationstechnik oder eine bestimmte Konfiguration informationstechnischer Einrichtungen

betreffend, es kann hierzu Geschäftsräume eines Betreibers von Kommunikationstechnik des Bundes innerhalb der üblichen Betriebs- und Geschäftszeiten betreten.

Einige dieser Vorschläge begegneten datenschutzrechtlicher Kritik, die ich während des Gesetzgebungsverfahrens – auch bei einer Anhörung des Innenausschusses des Deutschen Bundestags am 11. Mai 2009 – einbrachte (vgl. Kasten zu Nr. 5.2). Im Einzelnen sah ich folgende Punkte kritisch:

1. Das BSI erhält die Ermächtigung „Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen“ zu erheben und zu verarbeiten. Der Begriff der Protokolldaten war sehr weit gefasst und umfasste auch Verkehrsdaten gemäß TKG und Nutzungsdaten gemäß TMG. Eine Anonymisierung bzw. Pseudonymisierung dieser Daten vor der Auswertung war im Gesetz nicht gefordert, ebenso wenig ein weitgehender Verzicht auf die Herstellung eines direkten Personenbezugs. Die Aufgaben der Gefahrenabwehr und Beseitigung von Störungen erfordern keinen Personenbezug der Daten, eine Gefahrenabwehr kann auch durch ein weitgehend anonymes Scannen der Datenverkehre geschehen. Erforderlich ist aus der Sicht des Datenschutzes eine Verpflichtung zur Anonymisierung oder Pseudonymisierung. Eine Anonymisierung wäre zwar besser als eine Pseudonymisierung, aber es mag durchaus Fälle geben, in denen eine Pseudonymisierung erst das Erkennen und Verhindern von Angriffen ermöglicht. Gleichzeitig sollte nach dem Scannen eine sofortige Löschung erfolgen, wenn die Daten zur Erfüllung der Aufgabe – hier IT-Sicherheit, Abwehr von Angriffen – nicht mehr erforderlich sind, d. h. wenn der Scannvorgang keinen Hinweis auf eine Gefährdung erkennen lässt.

2. Das Gesetz sah von einer Benachrichtigungspflicht gegenüber den Betroffenen ab. Ich habe deshalb vorgeschlagen, grundsätzlich eine Benachrichtigungspflicht vorzusehen, von der nur in begründeten Einzelfällen abgewichen werden darf. Bei Erkennen von Angriffen oder Angriffsversuchen sollten grundsätzlich die davon Betroffenen unterrichtet werden.

3. Die Übermittlungsbefugnis des BSI war zu weit und erstreckte sich generell auch auf Straftaten, die mittels Telekommunikation begangen werden. Hier habe ich für die Einschränkung auf schwere Straftaten plädiert.

4. Die Erfassung und Auswertung von Daten aus dem Kernbereich privater Lebensgestaltung war an einen Prüfungsvorbehalt durch das BMI geknüpft. Dies entsprach nicht den Vorgaben des BVerfG. Daten aus dem Kernbereich privater Lebensgestaltung sind – wegen des hier einschlägigen verfassungsrechtlichen absoluten Verarbeitungsverbots – stets unverzüglich zu löschen, auch wenn anzunehmen ist, dass die Daten diesem Bereich zu zuordnen wären.

Insbesondere bei den parlamentarischen Verfahren fiel meine Kritik, die während der Anhörung auch von anderen Fachleuten geteilt wurde, auf fruchtbaren Boden.

Kasten zu Nr. 5.2

**IT-Sicherheit darf den Datenschutz nicht ausblenden**

**1. Stärkung der IT-Sicherheit darf nicht zu Lasten des Datenschutzes gehen**

Die Erhebung und Auswertung personenbezogener Daten muss ultima ratio sein. Angriffe auf die IT-Sicherheit können nicht nur die ordnungsgemäße Abwicklung von Diensten der Verwaltung und Wirtschaft beeinträchtigen, sondern auch Gefahren für die Persönlichkeitsrechte der Bürgerinnen und Bürger mit sich bringen. Daher sind Konzepte zu entwickeln und umzusetzen, die sowohl die IT-Sicherheit stärken als auch den Schutz der Privatsphäre gewährleisten.

In weiten Bereichen wurden in der jüngsten Vergangenheit Maßnahmen zur Stärkung der IT-Sicherheit getroffen, die eine detaillierte Registrierung und Auswertung des Nutzerverhaltens und sogar der Inhalte der Kommunikation ermöglichen. Die Datenschutzbeauftragten des Bundes und der Länder begrüßen zwar grundsätzlich alle Aktivitäten, um in den gewachsenen, vernetzten IT-Strukturen des Bundes das Niveau der IT-Sicherheit zu erhöhen. Sie fordern aber auch, dass die zur Risiko begrenzung eingeführten Maßnahmen nicht den Datenschutz der Nutzerinnen und Nutzer beeinträchtigen. Deshalb ist schon bei der Konzeption von IT-Sicherheitsmaßnahmen vorzusehen, dass das erforderliche Sicherheitsniveau nur mit datenschutzgerechten Lösungen gewährleistet wird. Ich fordere daher neben den strengeren Sicherheitsstandards zugleich die Möglichkeit, Protokoll- und Inhaltsdaten vor der Auswertung durch das BSI zu anonymisieren bzw. zu pseudonymisieren. Damit ließen sich eine unnötige Registrierung des Nutzerverhaltens und Überwachung von Kommunikationsinhalten vermeiden. Die Auswertung der Daten durch das BSI muss revisionssicher ausgestaltet werden.

**2. Anonymisierung und Pseudonymisierung bewusst einsetzen**

Anonymisierung und Pseudonymisierung können einen erheblichen Beitrag zu mehr Datenschutz und mehr IT-Sicherheit – nicht nur in den Netzen der Bundesverwaltung – leisten. Datenschutz und IT-Sicherheit stellen damit keinen Widerspruch dar, sondern ergänzen sich zum Wohle der Bürgerinnen und Bürger.

**3. Sicherheitslücken veröffentlichen!**

Bekannt gewordene Sicherheitslücken und Schadprogramme sind unverzüglich zu veröffentlichen, um damit Unternehmen und Bürger vor zu erwartenden Angriffen (Spionage und Sabotage) frühzeitig warnen zu können.

Das schließlich vom Deutschen Bundestag beschlossene BSI-Gesetz (BSIG) als Artikel 1 des Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14. August 2009 (BGBl. I S. 2821) trug meinen Bedenken und Forderungen weitgehend Rechnung. Nach dessen § 5 darf das BSI Protokolldaten und Schnittstellendaten in den Bundesnetzen zur Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes speichern und auswerten. Vor Aufnahme der Datenerhebung und -verwendung hat das BSI ein Datenerhebungs- und -verwendungskonzept zu erstellen und für Kontrollen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bereitzuhalten. Das Konzept hat dem besonderen Schutzbedürfnis der Regierungskommunikation Rechnung zu tragen. Die für die automatisierte Auswertung verwendeten Kriterien sind zu dokumentieren.

Ich habe im Berichtszeitraum – zunächst gemeinsam mit dem BSI – ein entsprechendes Konzept erarbeitet. Das Datenerhebungs- und Datenverwendungskonzept nach § 5 trägt den datenschutzrechtlichen Anforderungen Rechnung und dient der Transparenz der Verarbeitung der Daten beim BSI. Das Konzept unterliegt einer stetigen Anpassung an die veränderten Angriffs- aber auch Analysemethoden, sowie an die technischen Erfordernisse. Derzeit arbeitet das BSI an der technischen Umsetzung des Konzepts. Sobald es sich über einen längeren Zeitraum im Wirkbetrieb befindet, werde ich die Umsetzung kontrollieren und gegebenenfalls auf notwendige Modifikationen hinwirken.

### 5.3 Privacy Framework/technische Standardisierung

*Bei vielen technischen Vorgängen und Produkten sind datenschutzrechtliche Anforderungen zu erfüllen. Die Normung solcher Vorgänge oder Produkte muss deshalb auch diese Anforderungen berücksichtigen.*

Die Standardisierung von technischen Vorgängen hat in den letzten Jahren an Bedeutung gewonnen. Durch die Globalisierung der Märkte wächst auch bei Herstellern von Geräten und Anbietern von Dienstleistung die Nachfrage nach Standards mit weltweiter Gültigkeit. Viele technische Standards berühren auch Datenschutzaspekte, die allerdings allzu häufig erst im Nachhinein erkannt wurden. Deshalb habe ich mich – gemeinsam mit ausländischen Datenschutzbehörden und Landesdatenschutzbeauftragten – entschlossen, verstärkt bei ihrer Erarbeitung mitzuwirken. Dabei geht es sowohl um internationale Standards (insbesondere der ISO) als auch um deutsche Standardisierungsbemühungen durch das DIN.

So wirke ich derzeit bei der Überarbeitung der Norm DIN 32757 zur sicheren Vernichtung von Datenträgern mit. Sind personenbezogene Daten auf Datenträgern gespeichert, setzt ihre wirksame Löschung die sichere Vernichtung der Datenträger voraus. Die Miniaturisierung der Datenträger und die Zunahme der Informationsdichte (Anzahl von Bits pro Fläche) haben dazu geführt, dass die einschlägige DIN 32757 nicht mehr den Anforderungen der heute gängigen Technik genügt. Da Speichermedien immer preiswerter werden, sinkt vielfach der Anreiz, Daten zu löschen. Ich habe mich deshalb entschlossen, bei der Neuausrichtung dieser Regeln im Normenausschuss Informationstechnik und Anwendungen (NIA) „Arbeitsausschuss Vernichten von Datenträgern“ des Deutschen Instituts für Normung e. V. (DIN) mitzuarbeiten. Die seit 1995 bestehende DIN 32757 definiert Begriffe und legt Mindestanforderungen an Maschinen und Einrichtungen hinsichtlich der Vernichtung von Datenträgern in fünf Sicherstufensstufen fest. Die Sicherheitsstufen sind durch entsprechende Schnittbreiten und Schnittlängen charakterisiert. Diese Schnittbreiten, aber auch die Schnittlängen, orientieren sich an der Technik, die es damals am Markt gab.

So sind die Schnittbreiten beispielsweise beim Medium Papier an den gängigen Druckern und deren Schriftgrößen ausgerichtet. Bei den damals üblichen Matrixdruckern waren die Ergebnisse der Vernichtung durch Zerschneiden (Shreddern) gemäß den Sicherheitsstufen S1 bis S5 aus Datenschutzsicht durchaus tragbar. Dies gilt für heutige Drucker und Schriftgrößen nicht mehr. Durch Einsatz von kleineren besser lesbaren Schriften reduziert sich gleichzeitig auch der Papierverbrauch, sodass diese unter wirtschaftlichen Aspekten auch vermehrt eingesetzt werden. Bei der Vernichtung von Papier hat dies allerdings zur Folge, dass die aus der Norm übernommen Schnittbreiten nicht mehr den Datenschutzanforderungen genügen. Zum Teil sind längere Abschnitte auf den verbleibenden Papierschnipseln lesbar.

Das Gleiche gilt auch bei der Speicherung auf elektronischen Datenträgern. So vervierfacht sich die Informationsdichte bei der Verwendung einer DVD im Vergleich zu einer CD. Auch bei anderen Datenträgern führt die Miniaturisierung dazu, dass die Schnittbreiten bei der Vernichtung nicht mehr ausreichen. So hat eine klassische SD Memory Card eine Größe von 32 × 24 mm und wird somit noch durch die alte DIN 32757 erfasst, eine microSD mit 11 × 15 mm würde bei Verwendung der Stufen S1 bis S2 nicht mehr sicher vernichtet werden können, weil die Schnittbreite in der Norm zu groß ist.

Diese Beispiele zeigen, dass die Überarbeitung dringend notwendig ist, um den datenschutzrechtlichen Anforderungen schon bei der Entwicklung von Geräten Rechnung tragen zu können. Ein weiterer Gedanke, der bei der Vernichtung von Datenträgern berücksichtigt werden muss, ergibt sich aus der Frage des Recyclings des Vernichtungsgutes. Dabei gilt etwa folgende Regel: Je grober das Vernichtungsgut, umso besser die Recyclingmöglichkeiten. Diese Regel läuft allerdings den Datenschutzanforderungen entgegen, da größere Teilchen auch eine größere Informationsdichte umfassen. Einig sind sich aber alle Vertreter im Ausschuss, dass die alten fünf Stufen nicht mehr ausreichen und zumindest eine Stufe 6 in Zukunft erforderlich sein wird.

Die Gespräche dauern noch an und werden voraussichtlich im Frühjahr 2011 abgeschlossen sein. Ich bin optimistisch, dass die datenschutzrechtlichen Forderungen erfüllt werden.

## 5.4 Einmal erfasst – für immer gespeichert? Probleme mit der Datenlöschung

*Personenbezogene Daten müssen gelöscht werden, wenn sie nicht mehr erforderlich oder unzulässig gespeichert worden sind. Leider erfüllen nicht alle IT-Systeme diese rechtlichen Anforderungen.*

Die Software der Firma SAP unterstützt die Verwaltung von Waren, Dienstleistungen, aber auch von eigenem Personal oder Kundendaten. Auch die Bundesverwaltung nutzt diese Software immer häufiger zum Automatisieren von Geschäftsprozessen. Bei einigen Installationen hat sich gezeigt, dass personenbezogene Daten in SAP-Systemen nicht gelöscht werde können.

Nach dem Bundesdatenschutzgesetz sind personenbezogene Daten dann zu löschen, wenn sie für die Aufgabenerfüllung nicht mehr erforderlich sind oder ihre Speicherung aus anderen Gründen unzulässig ist. Das Gesetz definiert Löschen als Unkenntlichmachen gespeicherter personenbezogener Daten. Dies wird weder dadurch erreicht, dass die Daten nur logisch – mit der Möglichkeit einer Wiederherstellung – „gelöscht“ werden, noch dadurch, dass lediglich die Recherchemöglichkeit verhindert wird.

Leider habe ich bei verschiedenen Gelegenheiten feststellen müssen, dass Verfahren auf der Grundlage von SAP R/3 – insbesondere in der Personalverwaltung bei Einsatz des Moduls „HR“ (Human Resources Management) – den Anforderungen an eine datenschutzgerechte Löschung nicht genügen (hierzu vgl. auch unter Nr. 5.4.1 und 5.4.2). Ich habe dies zum Anlass genommen, mir einen groben Überblick über den Einsatz von SAP-Systemen in meinem Zuständigkeitsbereich zu verschaffen. Bei einer entsprechenden Umfrage habe ich Informationen zum Einsatz von SAP und der Art der in SAP-Systemen verarbeiteten personenbezogenen Daten (z. B. Kundendaten, Personaldaten, Beihilfedaten, Haushaltsdaten) gesammelt. Außerdem wollte ich wissen, ob ein Datenschutzkonzept erarbeitet wurde und eine Verfahrenanweisung existiert.

Beim Auswerten der Umfrage hat sich zunächst gezeigt, dass SAP nur in relativ wenigen Fällen in der Bundesverwaltung eingesetzt wird. Sofern allerdings das System benutzt wird, sind auch personenbezogene Daten betroffen, in vielen Fällen besonders schützenswerte Personalaktendaten und Personaldaten. Bei der Frage der Löschung personenbezogener Daten ergab sich ein bedenkliches Bild. Viele Behörden gingen bislang davon aus, dass die Daten innerhalb des Systems gelöscht werden können. Dass die SAP-Software dies nicht in allen Fällen leistet, war nicht allen bekannt. Erst durch meine Initiative scheint innerhalb der betroffenen Behörden ein Umdenken einzutreten und die vorhandene Löschroutine kritisch hinterfragt zu werden. Aufgrund des ernüchternden Ergebnisses der Umfrage – nicht in allen Fällen wird nach datenschutzrechtlichen Maßstäben richtig gelöscht – suchte ich das direkte Gespräch mit SAP, um mit dem Hersteller der Software Lösungswege zu finden. SAP sagte zu, im Laufe des Jahres 2010 ein Löschmodul bereitzustellen, das das Problem beseitigen könnte. Das Modul sei unter der Version SAP R/3 4.7 Enterprise ablauffähig. Die betroffenen Behörden haben das Modul inzwischen installiert und getestet. Der erwartete Erfolg hat sich jedoch nicht eingestellt. Das von SAP gelieferte Modul hat keine Löschungen vorgenommen und zum Teil zu Störungen in der Datenbank geführt. Die zu löschenden Daten sind in diesem Fall manuell gelöscht worden. Ich werde dies zum Anlass nehmen, das Problem im Frühjahr 2011 nochmals mit SAP intensiv zu beraten. Falls sich keine Änderung ergibt, werde ich dem Einsatz von SAP Produkten in Zukunft nicht mehr befürworten können.

### 5.4.1 Das Verfahren „oscare“ – neue elektronische Wege auch in der gesetzlichen Krankenversicherung

*Systembedingte datenschutzrechtliche Probleme bei dem von mehreren gesetzlichen Krankenkassen angewendeten Datenverwaltungsprogramm „oscare“ haben zu einer Reihe von Empfehlungen geführt.*

Das auf dem Programm SAP R/3 basierende Verfahren „oscare“ dient dazu, die Daten der Versicherten einer gesetzlichen Krankenkasse zu verwalten. Es wird – teilweise unter anderem Namen – mittlerweile von mehreren gesetzlichen Krankenkassen eingesetzt, die meiner Kontrolle unterliegen.

Um die datenschutzrechtlichen Anforderungen an dieses Verfahren zu prüfen, haben die Arbeitskreise Gesundheit und Soziales sowie Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter meiner Beteiligung die gemeinsame Arbeitsgruppe „oscare“ gebildet, um mit den gesetzlichen Krankenkassen und den entwickelnden Softwareunternehmen den Handlungsbedarf zu erörtern. Im Mittelpunkt dieser Erörterungen standen – wie bei anderen auf SAP R/3 basierten Verfahren – das Vorliegen eines Archivierungs- und Löschkonzeptes sowie die Protokollierung lesender Zugriffe. Zudem waren das Rollen- und Berechtigungskonzept und die Sicherstellung der Revisionsfähigkeit des Softwareeinsatzes, insbesondere durch eine geeignete Zugriffsprotokollierung, wesentliche Themen.

Festgestellt werden konnte, dass das bestehende Rollen- und Berechtigungskonzept grundsätzlich geeignet ist, den datenschutzrechtlichen Anforderungen gerecht zu werden. So lassen die im Verfahren bereitgestellten Einzelrollen die Einrichtung von Zugriffsberechtigungen in dem für die jeweilige Aufgabenerfüllung erforderlichen Umfang zu. Auch das Archivierungs- und Löschkonzept von „oscare“ genügt den Anforderungen der Datenschutzbeauftragten des Bundes und der Länder. Gleiches gilt für die zunächst nicht zufriedenstellende Protokollierung der lesenden Zugriffe. Hier soll das von dem Entwicklungsunternehmen der Software im August 2009 präsentierte zusätzliche Modul die revisionssichere und umfassende Protokollierung der aus dem Verfahren erzeugten Datenzugriffe gewährleisten.

Da sich im Laufe der Diskussion der Arbeitsgruppe zeigte, dass die datenschutzrechtlichen Anforderungen

nicht nur an das Verfahren „oscare“, sondern an alle vergleichbaren Verfahren zu stellen sind, hat die Arbeitsgruppe „Empfehlungen zur Protokollierung in zentralen IT-Verfahren der Gesetzlichen Krankenversicherung“ erarbeitet (vgl. Nr. 11.1.7).

### 5.4.2 Löschen von Beschäftigtendaten: Immer wieder Ärger mit SAP

*Bei zwei Beratungs- und Kontrollbesuchen in öffentlichen Stellen des Bundes musste ich feststellen, dass das eingesetzte Personalinformations- bzw. Personalverwaltungssystem von SAP über kein Löschkonzept für die gespeicherten Beschäftigtendaten verfügte.*

Bei meinem Beratungs- und Kontrollbesuch in der Leistungsabteilung der DRV Bund (vgl. Nr. 11.1.9) habe ich festgestellt, dass in dem dort eingesetzten Personalwirtschaftsverfahren (Personalinformationssystem SAP R/3 HR) krankheits- und urlaubsbedingte Abwesenheitszeiten der Beschäftigten zurückgehend bis zum Januar 2003 gespeichert waren – ein klarer Verstoß gegen die gesetzlichen Vorgaben des § 113 Absatz 2 Bundesbeamtengesetz (BBG), nach welchem die Unterlagen nach Ablauf der Aufbewahrungsfristen umgehend zu löschen sind. Leider hat sich gezeigt, dass es sich hierbei nicht um einen auf die Leistungsabteilung begrenzten Einzelfall, sondern um ein grundsätzliches Problem mit der eingesetzten Software handelt. Auch bei der Prüfung des Personalverwaltungssystems PVS BMVBS – einem konfigurierten und erweiterten SAP-HR-System – im Bundesamt für Seeschifffahrt und Hydrographie (BSH) und im Wasser- und Schifffahrtsamt Hamburg (WSA Hamburg) (vgl. Nr. 12.4) war die Löschung personenbezogener Daten nicht möglich. Im Gegensatz zu meinem Befund bei der DRV Bund waren die Aufbewahrungsfristen bei der Mehrzahl der im Personalverwaltungssystem PVS BMVBS gespeicherten Personalaktendaten zum Kontrollzeitpunkt allerdings noch nicht abgelaufen, so dass ein Verstoß gegen die gesetzliche Löschungspflicht nicht festgestellt werden konnte.

Die DRV Bund habe ich zur unverzüglichen Löschung aller unzulässig gespeicherten Personalaktendaten aufgefordert. Inzwischen hat mir die DRV Bund mitgeteilt, dass SAP ein überarbeitetes Modul zur Löschung von Abwesenheiten entwickelt hat, das demnächst von der DRV Bund eingesetzt werden kann. Ich werde die Angelegenheit weiter verfolgen und mir den angesprochenen Löschreport von SAP in der Hauptstelle der DRV Bund zeitnah vorführen lassen.

Für das Personalverwaltungssystem PVS BMVBS hat mir das zuständige Bundesministerium für Verkehr, Bau und Stadtentwicklung (BMVBS) mitgeteilt, dass die von SAP standardmäßig angebotenen Löschreports auch in einer neueren Version nicht uneingeschränkt einsetzbar gewesen seien. Das BMVBS hat daraufhin eine externe Firma mit der Neuentwicklung eines zusätzlichen Löschreports beauftragt und alle nicht mehr erforderlichen personenbezogenen Daten der Beschäftigten manuell gelöscht. Das BMVBS hat mir zugesichert, dass die Löschung der in PVS BMVBS gespeicherten personenbezogenen Daten zukünftig routinemäßig nach festen Zeitplänen erfolgen wird. Auch das BMVBS werde ich bei dem Einsatz des Personalverwaltungssystems PVS BMVBS weiterhin unterstützen (zu den technischen Anforderungen an Systeme mit denen personenbezogene Daten verarbeitet werden, vgl. Nr. 5.4). Unterstreichen möchte ich an dieser Stelle, dass die Zusammenarbeit mit dem BMVBS sehr kooperativ verlief.

## 5.5 Einführung der elektronischen Personalakte bei der DRV Bund

*Die DRV Bund hat bei der geplanten Einführung der elektronischen Personalakte zahlreiche meiner Empfehlungen aufgegriffen. In einigen Bereichen besteht jedoch noch Handlungsbedarf.*

Nachdem es nunmehr nach dem Bundesbeamtengesetz (BBG) zulässig ist, die Personalakten der Beamtinnen und Beamten des Bundes automatisiert zu führen (vgl. Nr. 12.3), hat mir die DRV Bund in mehreren Beratungsgesprächen ihre Planungen zur Einführung einer elektronischen Personalakte vorgestellt. So ist geplant, das Personalwirtschaftsverfahren der DRV Bund um das Teilverfahren ePersonalakte („elektronische Personalakte“) zu erweitern und die elektronischen Dokumente in einem zentralen Dokumentenmanagementsystem manipulationssicher abzulegen. Meine datenschutzrechtlichen Empfehlungen und Hinweise zu der hausinternen Richtlinie zur elektronischen Personalakte und zu einem Handlungsleitfaden hat die DRV Bund aufgegriffen.

Auch habe ich weitere Maßnahmen im Verfahren „elektronische Personalakte“ – auch in technischer und organisatorischer Hinsicht – empfohlen, die eine datenschutzgerechte Verfahrensweise in Zukunft ermöglichen. Dies gilt insbesondere für die Löschung von personenbezogenen Daten, aber auch für die Sicherstellung des Einsichtsrechtes der Betroffenen nach § 110 Absatz 1 BBG.

Vor der Einführung muss allerdings die noch offene Frage des „manipulationssicheren“ Einscannens von Personalaktendaten datenschutzgerecht gelöst werden. Bei einer ersten Präsentation des vorgesehenen Scanprozesses hatte sich gezeigt, dass die DRV Bund bisher hinsichtlich der zu scannenden Originalbelege aus der Personalakte keine schriftliche Regelungen getroffen hatte. Derartige Regelungen sind aber beispielsweise für die Fälle notwendig, dass Original-Personalaktendaten während des Scanprozesses beschädigt oder zerstört werden oder ein Original-Dokument nach dem Einscannen verloren geht und dies erst später bei der Aktenbearbeitung oder Prüfung festgestellt wird. Ich habe der DRV Bund empfohlen, verbindlich festzulegen, wer in solchen Fällen und in welcher Form weitere Maßnahmen einleiten bzw. Entscheidungen treffen muss. Die Fehlerfälle sind – für den Betroffenen und den Datenschutzbeauftragten nachvollziehbar – schriftlich zu dokumentieren. Die DRV Bund hat mir zugesagt, entsprechende Verfahrensbeschreibungen zu erstellen, die denkbare Fehlerfälle im Scanprozess und das weitere Vorgehen in solchen Fällen verdeutlichen.

Aufgegriffen hat die DRV Bund meine Empfehlungen, das Scannen und Signieren der Bestandspersonalakten und die Digitalisierung neuer Vorgänge in einem gesonderten Bereich der Scanstelle ausschließlich durch Beschäftigte der Personalabteilung durchführen zu lassen.

Ich sehe allerdings noch weiteren Handlungsbedarf. Die DRV Bund ist als personalaktenführende Stelle für die Eindeutigkeit, Vollständigkeit und Richtigkeit der Personalakte verantwortlich. Allerdings plant die DRV Bund bislang, lediglich 2 Prozent der eingescannten Originalunterlagen stichprobenartig auf ihre Richtigkeit zu überprüfen und mit einer elektronischen Signatur zu versehen. Die rudimentäre Prüfung erscheint problematisch, weil die Originalunterlagen nach dem Scannen in absehbarer Zeit vernichtet werden müssen, um eine dauerhafte parallele Führung gleicher Aktenteile in Papierform und in elektronischer Form zu vermeiden. Damit die DRV Bund zu jeder Zeit – also auch nach Vernichtung der Papierdokumente – in der Lage ist, die Eindeutigkeit, Richtigkeit und Übereinstimmung der elektronischen Dokumente mit den früheren Papier-Originalen nachzuweisen, muss also jedes einzelne elektronische Dokument nach dem Einscannen und vor der Vernichtung der Originalunterlage geprüft und anschließend mit einer qualifizierten digitalen Signatur versehen werden.

Für die Prüfung, inwiefern für die Umsetzung der gesetzlichen Vorgaben des BBG ein Übergangszeitraum gewährt werden kann, hat die DRV Bund auf meine Anregung eine Stellungnahme des Bundesministeriums des Innern (BMI) eingeholt. Darin führt das BMI aus, dass die bereits eingescannten Bestandsakten nicht aus allgemeinen Sicherheitserwägungen dauerhaft vorgehalten werden dürfen. Zugleich hat es aber dargelegt, unter welchen Voraussetzungen ein zeitlich begrenztes Vorhalten der Papierakten nach dem Einscannen zu Kontrollzwecken sachlich gerechtfertigt ist. Insbesondere müssen nach der Durchführung des Massenscanverfahrens alle zumutbaren Maßnahmen ergriffen werden, die eine kontinuierliche Verringerung der vorgehaltenen Papierakten ermöglichen. Eine Sichtkontrolle müsse daher laufend – und nicht nur anlassbezogen – durchgeführt werden, damit zumindest nach absehbarer Zeit auf die Papierakten verzichtet werden könne.

Da ich die Rechtsauffassung des BMI teile, habe ich gegenüber der DRV Bund eine vollständige Sichtprüfung mit qualifizierter digitaler Signatur der eingescannten Papierakten und anschließender Vernichtung der Papierakten „nach und nach“ angeregt. Die DRV Bund prüft derzeit meinen Lösungsvorschlag, hat aber darauf hingewiesen, dass die vollständige Prüfung der digitalisierten Dokumente zu einer erheblichen Mehrbelastung führen wird. Zugesagt hat mir die DRV Bund bereits, dass bei der Digitalisierung künftiger, also neuer Vorgänge das Anbringen der Signatur mit einer 100-prozentigen Sichtprüfung erfolgen wird.

Ich werde die DRV Bund bei der Einführung der elektronischen Personalakte – der ich grundsätzliche Bedeutung beimesse – weiterhin beratend unterstützen und den Umsetzungsprozess aufmerksam beobachten.

## 5.6 Cloud Computing – Datenschutz in der Wolke?

*Das Bereitstellen von Rechenkapazitäten über das Internet im Rahmen des sog. Cloud Computing wirft viele datenschutzrechtliche Fragen auf.*

Cloud Computing bezeichnet das dynamische Bereitstellen von Ressourcen wie Rechenkapazitäten, Datenspeicher oder fertiger Programmpakete über Netze, insbesondere über das Internet. Für das Cloud Computing wird mit möglichen Kosteneinsparungen und größerer Flexibilität geworben. Hierbei stellt sich jedoch die Frage, wie der Datenschutz und die Datensicherheit gewährleistet werden können.

Cloud Computing in seiner Reinform – als ein offenes, globales Modell – ist mit dem geltenden Datenschutzrecht schwer in Einklang zu bringen. Entschließt sich eine verantwortliche Stelle, also der Auftraggeber von Cloud-Diensten, personenbezogene Daten auf verteilten Rechnern weltweit speichern zu lassen, stößt dieser Ansatz schnell an seine Grenzen. Im Extremfall weiß die verantwortliche Stelle nicht einmal, wo und von wem die Daten technisch verarbeitet werden. Es muss daher einschränkende Bedingungen beim Einsatz des Cloud Computing geben.

Da die Auftraggeber in der Mehrzahl der Konstellationen die Verantwortung für ihre Daten nicht aus der Hand geben wollen, handelt es sich sowohl nach der europäischen Datenschutzrichtlinie als auch nach dem Bundesdatenschutzgesetz um eine Form der Auftragsdatenverarbeitung. Damit verbleibt nach § 11 BDSG auch die datenschutzrechtliche Verantwortung in aller Regel bei der verantwortlichen Stelle. Daraus ergibt sich, dass eine Reihe von rechtlichen, formalen sowie technischen und organisatorischen Anforderungen zu berücksichtigen sind (vgl. auch Nr. 2.4 zur Auftragsdatenverarbeitung). Beim Cloud Computing ist u. a. Folgendes zu beachten:

Die Verlagerung der Verarbeitung in die Cloud darf grundsätzlich nur dann erfolgen, wenn eine Delegation von Datenverarbeitungsvorgängen an private Dritte im Sinne einer Auftragsdatenverarbeitung zulässig ist. Dabei sind die bereichsspezifischen Grenzen – etwa des Sozialrechts – zu beachten.

In der Regel macht die Verarbeitung in der Cloud nicht an den deutschen Grenzen halt. Die Auftragsvergabe an ausländische Auftragnehmer unterliegt nur dann den gleichen Anforderungen wie in Deutschland, wenn der Auftragnehmer seinen Sitz in der EU oder in Ländern des Europäischen Wirtschaftsraums (EWR) hat oder die Daten zumindest in deren Gebiet verarbeitet werden.

Für Auftragnehmer, die Daten außerhalb der EU oder des EWR verarbeiten, muss zusätzlich ein angemessener Datenschutz in den jeweiligen Drittstaaten gewährleistet und ggf. eine Genehmigung bei der für die verantwortliche Stelle zuständige Datenschutzbehörde eingeholt werden. An die Angemessenheit der Maßnahmen sind dieselben Anforderungen zu stellen wie bei der Datenübermittlung in einen Drittstaat.

Die in § 11 BDSG festgelegten Anforderungen sind sowohl bei Vergabe an inländische wie an ausländische Auftragnehmer zu beachten. So muss der schriftliche Auftrag beispielsweise Gegenstand und Dauer, den Umfang, die Art der Daten und den Kreis der Betroffenen, die technischen und organisatorischen Maßnahmen, Regelung der Berichtigung und Löschung und weitere Festlegungen nach § 11 Absatz 2 BDSG enthalten. Dies setzt voraus, dass der Auftraggeber im Detail weiß, welche der Daten wo unter welchen Bedingungen verarbeitet werden. Dies ist bei Cloud Computing dann schwer zu bewerkstelligen, wenn freie Serverkapazitäten erst ad hoc zugewiesen werden.

Der Auftraggeber muss sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der technisch-organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes überzeugen. Dies kann durch eine Vor-Ort-Inspektion geschehen oder durch Zertifizierung durch einen unabhängigen und vertrauenswürdigen Dritten, der kein eigenes Interesse an einer positiven Zertifizierung hat. Auf jeden Fall sind dabei die Bedingungen der im Einzelnen genutzten Rechenzentren und deren Bedingungen vor Ort einzubeziehen.

Eine wirksame Datenschutzkontrolle muss auch beim Auftragnehmer gewährleistet sein. Auch hier dürften sich angesichts des verteilten Ansatzes diverse praktische Schwierigkeiten ergeben.

Aus den genannten Gründen ist das Cloud Computing derzeit nur unter eingeschränkten Bedingungen zulässig und praktikabel.

Ein Lösungsansatz wäre z. B. eine Vorschrift zur gemeinsamen Datenverarbeitung mehrerer verantwortlicher Stellen. Möglicherweise kann auch das Konzept der nachhaltigen Verantwortlichkeit („Accountability“) in dieser Richtung hilfreich sein. Accountability bedeutet, die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung bei der Beteiligung mehrerer Stellen durch entsprechende Vorschriften von den tatsächlichen Einflussmöglichkeiten und der Interessenlage der Betroffenen abhängig zu machen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu in ihren Eckpunkten zur Modernisierung des Datenschutzrechts bereits erste Vorschläge unterbreitet (vgl. Nr. 1).

Erforderlich ist eine interessengerechte Verteilung der Verantwortlichkeiten, d. h. beim Cloud Computing auch des oder der Auftragnehmer(s). Jede Stelle, die in tatsächlicher Hinsicht über Mittel und Zwecke der Datenverarbeitung verantwortlich bestimmen kann, soll in diesem Umfang auch verantwortlich für die Rechtmäßigkeit der Datenverarbeitung sein.

Nur wenn bestimmte rechtliche, technische und organisatorische Voraussetzungen erfüllt sind, sollten Dienstleitungen über eine Cloud realisiert werden (vgl. Kasten zu Nr. 5.6). Personenbezogene Daten dürfen nur dann in der Cloud verarbeitet werden, wenn sie effektiv gegen Missbrauch geschützt werden. Hierzu sollte auch dem Grundsatz des Privacy by Design gefolgt werden, um frühzeitig, bereits bei der Erstellung von Cloud-Services, einen effektiven Datenschutz zu implementieren. Zudem sollte ein Höchstmaß an Transparenz bei der Inanspruchnahme von Cloud-Diensten gewährleistet sein. Insgesamt sehe ich beim Cloud Computing noch viele offene rechtliche und technische Fragen.

Kasten zu Nr. 5.6

Zum Einsatz von Cloud Computing befindet sich ein Leitfaden „BSI-Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter“ in der öffentlichen Abstimmung. In diesem Dokument (Version 0.96 vom 27. September 2010) werden Basisanforderungen, Anforderungen an hohe Vertraulichkeit und hohe Verfügbarkeit auf Grundlage des IT-Grundschutzes beim Einsatz von Cloud Computing aufgeführt. Betrachtet werden hier u. a. das Sicherheitsmanagement beim Anbieter, Sicherheitsarchitektur, ID- und Rechtemanagement, Transparenz, organisatorische Anforderungen, Kontrollmöglichkeiten für den Nutzer und Datenschutz/Compliance. Mit Hilfe des Leitfadens soll ein so komplexes Thema wie der Einsatz von Cloud Computing unter IT-Sicherheitsgesichtspunkten für Anbieter von Cloud Diensten ermöglicht werden.

## 5.7 Ohne Vollprotokollierung keine „Waffen“-Gleichheit!

*Ohne eine umfassende Vollprotokollierung, d. h. eine Protokollierung aller Datenbanktransaktionen und deren Inhalte, und die automatisierte Auswertung dieser Daten ist eine angemessene und effiziente Datenschutzkontrolle bei den Sicherheitsbehörden vielfach nicht mehr möglich.*

Die Sicherheitsarchitektur hat sich in den letzten Jahren gravierend verändert (vgl. Nr. 7.1). Hervorzuheben ist die zunehmende informationelle Vernetzung der Sicherheitsbehörden und die Errichtung zentraler Großdateien mit enormen Datenmengen. Zudem werden zunehmend Datenbanken fusioniert bzw. neue gemeinsame Datenbanken, wie z. B. die Antiterrordatei in Deutschland (vgl. 21. TB Nr. 5.1.1), geschaffen, in denen die Daten von Polizeien und Geheimdiensten zusammenfließen.

Hieraus resultieren neue Herausforderungen für den Datenschutz. Die riesigen Datenmengen müssen effizient und sachgerecht kontrolliert werden können. Dies ist aber vielfach nur möglich, wenn zum Zweck der Datenschutzkontrolle alle Transaktionen (z. B. jede Speicherung, Löschung, Änderung, Übermittlung) und deren Inhalte protokolliert werden (sog. Inhalts- und Transaktionsvollprotokollierung). Ohne eine derartige Protokollierung sind oftmals komplexe Bearbeitungsvorgänge, insbesondere in Datenbanken, in denen viele Behörden große Datenmengen gemeinsam verarbeiten, durch die Datenschutzkontrollorgane in Gänze, d. h. lückenlos von Anfang bis Ende, kaum bzw. nur mit extremen Aufwand überprüfbar. Dies betrifft beispielsweise die Frage, welche Behörde wann, welches (Teil-)Datum gespeichert, wie sie es bzw. wann sie es verarbeitet bzw. mit welchem Inhalt an andere Behörden übermittelt hat und ob dieses Datum als Teil eines neuen Datensatzes von der Empfängerbehörde erneut in

der Sicherheitsdatei gespeichert worden ist. Wie bei der Antiterrordatei bereits praktiziert, muss eine derartige Vollprotokollierung revisionssicher in einer gesonderten Protokolldatei (Protokolldatenbank) erfolgen.

Durch eine derart umfassende Vollprotokollierung werden die in den sicherheitsbehördlichen Dateien vorhandenen Daten in die entsprechenden Protokolldatenbanken dupliziert. Infolgedessen können Daten, die in den Sicherheitsdateien zwischenzeitlich gelöscht worden sind, in den Protokolldatenbanken noch vorhanden sein. Um die hiermit verbundenen Risiken zu minimieren, sind besondere Sicherungsmaßnahmen erforderlich. Durch eine strenge Zweckbeschränkung der Protokolldaten ist zu gewährleisten, dass die Daten nur für Kontrollzwecke verwendet werden dürfen. Zudem ist die Speicherdauer der Protokolldaten angemessen zu begrenzen, um ein Fortbestehen der Datenbestände auf den für die Kontrollzwecke notwendigen Zeitraum zu beschränken.

In Folge einer derartigen Vollprotokollierung entstehen unvermeidlicherweise extrem umfängliche Protokolldatenbanken. Derartige Datenmengen können sachgerecht oftmals nur mit technischen Hilfsmitteln ausgewertet werden. Erforderlich ist der Einsatz von Auswerteprogrammen, die die Kontrollorgane in die Lage versetzen, die Datenmengen schnell und einfach zu strukturieren bzw. nach bestimmten Merkmalen und Vorgaben auszuwerten. Diese Auswertetools müssen von den Sicherheitsbehörden bereits bei der Erstellung der Datenbanken konzeptionell eingeplant bzw. in vorhandene Datenbanken technisch eingefügt werden.

Ich habe die Bundesregierung aufgefordert, entsprechende Protokollierungssysteme für die bei den Sicherheitsbehörden des Bundes betriebenen Datenbanken vorzusehen. In der Antiterrordatei wird dies bereits umgesetzt. Auch in andere große, neue Datenbanksysteme der Sicherheitsbehörden sollen derartige Auswertungsmöglichkeiten integriert bzw. planerisch berücksichtigt werden, z. B. im Rahmen der Neukonzeption des nachrichtendienstlichen Verbundsystems der Verfassungsschutzbehörden des Bundes und der Länder (NADIS-NEU – vgl. Nr. 7.5.1).

Das Bundeskanzleramt hat sich in Bezug auf die vom Bundesnachrichtendienst geführten Dateien ablehnend geäußert. Es erachtet eine derartige Protokollierung als nicht angemessen. Insbesondere der finanzielle Aufwand hierfür sei zu groß. Ich habe das Bundeskanzleramt darauf hingewiesen, dass sich die Beurteilung der Angemessenheit – und damit der Verhältnismäßigkeit – im Sinne des § 9 Satz 2 BDSG nach den Schutzzwecken bzw. -bedürfnissen der verarbeiteten Daten bemisst. Je höher das Schutzbedürfnis dieser Daten ist, desto höher ist der Aufwand, den das Bundesdatenschutzgesetz der verantwortlichen Sicherheitsbehörde zumutet. Dies gilt insbesondere bei der Verarbeitung von besonders sensiblen Daten, d. h. von Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben. Auch derartige Daten werden von den Sicherheitsbehörden verarbeitet.

Ein angemessener Protokollierungsaufwand ist auch deshalb erforderlich, weil eine fehlerhafte Verarbeitung für den Betroffenen nicht sofort erkennbar ist und die daraufhin getroffenen Entscheidungen der Sicherheitsbehörden für ihn nur schwer überprüfbar oder revidierbar sind. Dies ist bei den Sicherheitsbehörden vielfach der Fall, da sie die Daten der Betroffenen oftmals – bei den Nachrichtendiensten sogar in aller Regel – heimlich, d. h. ohne die Kenntnis der Betroffenen erheben und verarbeiten – mit potentiell gravierenden Folgen für die Betroffenen.

Die Beratungen hierzu dauern an.

## 5.8 Elektronische Fahrzeugdatenspeicher – das Auto als rollender Computer

*Elektronische Fahrzeugdatenspeicher in PKW sollen die Sicherheit des Fahrzeugs erhöhen und die Wartung erleichtern. Gleichzeitig steigt aber auch das Risiko, dass am Ende der Entwicklung der „gläserne Autofahrer" stehen könnte.*

Nach bescheidenen Anfängen vor etwa 30 Jahren werden PKW heute mit immer komplexeren und leistungsfähigeren elektronischen Helfersystemen und Datenspeichern ausgerüstet, deren Existenz und Funktionsweise Haltern und Fahrern wenig oder gar nicht bekannt sind. Manche der dabei anfallenden Daten haben zunächst gar keinen Personenbezug, wie etwa Daten des technischen Motormanagements. Kommen allerdings weitere, unmittelbar verhaltensbedingte Informationen hinzu, wird die Schwelle zur Personenbeziehbarkeit schnell erreicht. Dies gilt etwa für die Häufigkeitsverteilung von Messwerten zur Geschwindigkeit, (Quer-) Beschleunigung, Fahrzeugposition sowie zum Bremsverhalten und hierbei aufgetretenen Verzögerungswerten.

Ein handelsüblicher PKW enthält zwischen 40 und 60 mit einem Datenleitungssystem verbundene Fahrzeugdatenspeicher. Dort gespeicherte Daten können von Werkstätten und Herstellern von einem zentralen Abruf-Steckplatz aus abgerufen werden. Zu Wartungsarbeiten genutzte Daten informieren etwa über das Beschleunigungs-, Geschwindigkeits- und Bremsverhalten des Fahrers. Damit entsteht ein detailliertes Nutzungs- und ggf. auch Fahrerprofil. Kommen noch Online-Daten, wie etwa. eine Lokalisierung über GPS hinzu, rückt der „gläserne Autofahrer" immer näher.

Die Nutzung dieser Daten durch Werkstätten zur Erfüllung von Wartungs- und Reparaturaufträgen des Halters ist dann zulässig, wenn er sich vor der Auftragserteilung durch schriftliche Hinweise in der Betriebsanleitung, im Kaufvertrag seines PKW oder im Wartungs- oder Reparaturvertrag über die im Fahrzeugdatenspeicher vorhandenen Informationen nachvollziehbar informieren kann und er zugleich Fahrer des entsprechenden PKW ist. Gleiches gilt für die Erhebung, Verarbeitung und Nutzung von Fahrzeugdaten aus dem „Schattenspeicher" des PKW, auf den nur der Hersteller zugreifen kann.

Eine nachvollziehbare Information im obigen Sinn liegt nicht vor, wenn sie sich auf pauschale Hinweise beschränkt, wie etwa: „Ihr Fahrzeug zeichnet Daten über

den Betrieb, Fehler und Benutzereinstellungen auf. Diese Daten werden im Fahrzeug gespeichert und können mit geeigneten Geräten, insbesondere im Service, ausgelesen werden. Die ausgelesenen Daten werden für die Unterstützung der Serviceprozesse, zur Reparatur oder zur Optimierung und Weiterentwicklung von Fahrzeugfunktionen verwendet."

Der Düsseldorfer Kreis hat die datenschutzrechtlichen Probleme elektronischer Fahrzeugdatenspeicher aufgegriffen und eine Arbeitsgruppe eingerichtet, an der ich mitarbeite. Die Arbeitsgruppe hat zunächst die Datenerhebung, -verarbeitung und -nutzung der Fahrzeugdaten mit Blick auf ihren Personenbezug untersucht. Ziel dieser Analyse ist es, die Information der Betroffenen in Betriebsanleitungen, Kaufverträgen sowie bei Wartungs- und Reparaturaufträgen zu verbessern. Die hierfür erforderlichen Arbeiten waren bei Redaktionsschluss noch nicht abgeschlossen.

## 5.9 RFID PIA auf europäischer Ebene

*Um beim Einsatz von RFID (Radio Frequency Identification) Datenschutzbedrohungen und Auswirkungen zu untersuchen, wurde auf europäischer Ebene ein Konzept zur Datenschutzfolgenabschätzung – Privacy Impact Assessment (PIA) – entwickelt. Zukünftig sollen PIA Reports von der RFID einsetzenden Industrie, dem Handel und der Wirtschaft erstellt und den nationalen Aufsichtsbehörden vor Inbetriebnahme zur Prüfung vorgelegt werden.*

RFID ist unaufhaltsam dabei, die Welt zu erobern. Dies geschieht zumeist im Verborgenen und unsichtbar für den Bürger. So sind mittlerweile RFID-Chips in Kleidungsstücken namhafter Hersteller oder etwa in Kundenkarten oder dem neuen Personalausweis integriert. Zur Kennzeichnung von mit RFID versehenen Produkten empfiehlt etwa das Informationsforum RFID ein aus einem Ideenwettbewerb hervorgegangenes RFID Logo (vgl. Kasten a zu Nr. 5.9). Auch alle Pässe mit RFID-Chips nach dem ICAO-Standard sind mit einem Logo (vgl. Kasten b zu Nr. 5.9) gekennzeichnet. Zum Thema RFID hatte ich bereits in meinen letzten Tätigkeitsberichten (vgl. zuletzt 22. TB Nr. 6.7) ausführlich informiert.

Das Konzept der EU-Kommission sieht die Entwicklung eines Prüfleitfadens zur Technikfolgenabschätzung beim Einsatz von RFID-Systemen (RFID PIA) vor. Die Entwicklung eines RFID PIA geht zurück auf die Empfehlung der EU-Kommission vom 12. Mai 2009 2009/387/EG (L 122 S. 47), nach der mehrere Grundsätze beim Einsatz von RFID zu beachten sind.

Hierzu gehören:

– Die spezielle Kennzeichnung von mit RFID versehenen Waren.

– Der Hinweis auf den Einsatz von RFID mittels eines europaweit einheitlichen Logos.

– Allgemeine Information zum Einsatz von RFID.

– Die automatische Deaktivierung der Funkchips beim Verlassen der Ladenkasse.

Nur auf ausdrücklichen Wunsch des Käufers nach dem Opt-In Prinzip sollen RFID weiterhin nach der Bezahlabwicklung funken dürfen. RFID-Schreib-/Lesegeräte sowie Kommunikationsvorgänge sollten für den Kunden eindeutig erkennbar sein. Es sollte umfassend darüber informiert werden, welche personenbezogenen Daten beim Einsatz zu welchem Zweck verarbeitet werden.

Vor der Verwendung sollen eingesetzte RFID-Systeme mittels Folgenabschätzungen auf ihre Vereinbarkeit mit den datenschutzrechtlichen Anforderungen untersucht werden. Zudem sollte mindestens sechs Wochen vor Inbetriebnahme der Systeme den nationalen Datenschutzbehörden ein Bericht zur Prüfung vorgelegt werden. Mit dieser (nicht bindenden) Empfehlung, welche auf eine Online-Konsultation aus dem Jahre 2006 zurück geht, sollen europaweit gleiche Ausgangsbedingungen bei Herstellern und Anwendern von RFID geschaffen werden.

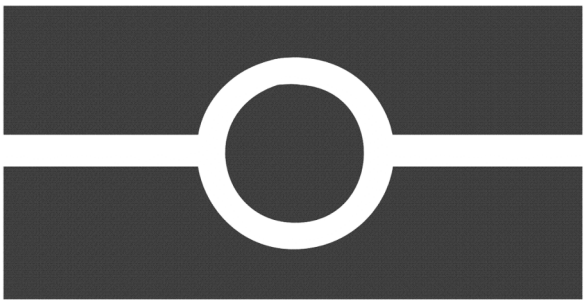
Die Artikel-29-Gruppe der Datenschutzbeauftragten der EU-Staaten hat ein von Vertretern der Industrie im März 2010 vorgelegtes Papier zum RFID PIA als nicht ausreichend angesehen (Arbeitspapier 175 vom 13. Juli 2010). Kritisiert wurde insbesondere, dass das PIA nicht nur Technik beschreiben solle, sondern ihre Risiken identifizieren müsse. Ferner sei die Betrachtung von solchen RFID unterblieben, die von Personen mitgeführt werden. Schließlich fehle auch die aus Datenschutzsicht wichtige Untersuchung der Deaktivierbarkeit der Funkchips am Verkaufsort. Seitdem befindet sich das unter Federführung der GS1/Retail (Global Standards One) entwickelte RFID PIA in der Überarbeitung. Neuere, jedoch ebenfalls noch verbesserungsbedürftige Versionen wurden der Artikel-29-Gruppe zur Begutachtung zugeleitet. Diese Versionen enthalten gegenüber der ersten Fassung deutliche Verbesserungen. Eine finale Vorlage der Industrie wurde mittlerweile eingereicht. Diese wurde durch eine Stellungnahme der Artikel-29-Gruppe positiv bewertet und offiziell angenommen. Damit würde das RFID PIA in den Mitgliedstaaten der EU zukünftig die Einhaltung von einheitlich hohen Datenschutzanforderungen beim Einsatz von RFID ermöglichen.

Kasten a zu Nr. 5.9

RFID-Logo zur Kennzeichnung von Produkten

Kasten b zu Nr. 5.9

RFID-Logo zur Kennzeichnung von Pässen



## 5.10 THESEUS – neue Technologien für das Internet der Dienste

*Im Rahmen des vom BMWi geförderten Kooperationsprojekts THESEUS zur Erforschung neuer Internettechnologien konnte ich datenschutzrechtliche Verbesserungen erreichen.*

Im Rahmen des IT-Gipfels 2006 beschloss die damalige Bundesregierung, das Forschungsprogramm THESEUS zu fördern. Ursprünglich startete das mittlerweile größte deutsche IT-Forschungsprogramm im Bereich semantischer Suchmaschinen mit dem Ziel der Entwicklung neuer Suchtechnologien für das Internet. Unter semantischen Suchmaschinen versteht man Suchmaschinen, die die Bedeutung der Eingabe analysiert und in einem Datenbestand nach passenden Antworten sucht. Mittlerweile hat sich der Schwerpunkt hin zur Bereitstellung und Vernetzung von Daten und Wissen sowie der Entwicklung neuer Internet-Dienstleistungen verlagert.

Ich begleite das THESEUS Programm bereits seit 2007. Im Jahre 2008 wurde mir ein erster Bericht vorgelegt, in welchem die datenschutzrechtliche Ausgestaltung des Projektes dargestellt werden sollte. Der Bericht nahm sich des Themas jedoch nur peripher ohne ein schlüssiges Konzept an und warf stattdessen neue datenschutzrechtliche Fragen auf. Er beschrieb verschiedene Anwendungsszenarien, unter anderem die Analyse medizinischer Daten oder den Entwurf neuartiger Internet-Plattformen. Auf mein Drängen und nach einigen Koordinationsschwierigkeiten wurden schließlich im Jahr 2010 ausführliche Gespräche mit Vertretern des BMWi und der Industrie geführt.

Innerhalb der Diskussionen konnte ich die Projektleitung davon überzeugen, dass gerade bei medizinischen Daten ein hoher Datenschutzstandard gewährleistet sein muss. Bisher existiert allerdings keinerlei Überblick, ob und welche personenbezogenen Daten in den verschiedenen Anwendungsszenarien erhoben und verarbeitet werden.

Als ein Ergebnis der Gespräche wurde auf meinen Vorschlag ein Fragenkatalog zum Thema „Datenschutz in THESEUS“ erstellt und den verschiedenen Industriepartnern zugeleitet. Dessen Auswertung führte zu einer Identifikation von aus datenschutzrechtlicher Sicht relevanten Anwendungsszenarien.

Aus meiner Sicht sind in vielen Anwendungsszenarien inzwischen ausreichende Datenschutzmaßnahmen vorgesehen. So beschäftigen sich die im medizinischen Bereich angesiedelten Teilprojekte MEDICO und RADMINING mit der Analyse radiologischer Daten und Befunde. Hier werden Pseudonymisierungsverfahren für personenbezogene Daten eingesetzt, eine strikte Zugangsregelung für sensible Daten vorgenommen und in Zusammenarbeit mit innerbetrieblichen Datenschutzbeauftragten und den beteiligten Ärzten auf die Einhaltung des Datenschutzes und der ärztlichen Schweigepflicht strikt geachtet.

Allerdings haben sich auch einige kritische Punkte gezeigt. Dazu zählen die unnötige Zwischenspeicherung sensibler Daten vor der Pseudonymisierung oder die fehlende Zweckbindung bei der Speicherung von Verkehrsdaten der Telekommunikation. Die größten Bedenken habe ich beim Anwendungsszenario ALEXANDRIA, in dem eine Internet-Plattform zum Austausch von Wissen entwickelt wird. Hier besteht noch erheblicher Nachbesserungsbedarf, um Profilbildungen, Missbrauch von Daten, den externen Zugriff auf Daten zu unterbinden. Das hier vorgesehene Konzept der Selbstregulierung halte ich nicht für ausreichend und habe deshalb Verbesserungen gefordert.

Ich werde das THESEUS-Programm, auch im für 2011 und 2012 anvisierten Echtbetrieb, weiterhin begleiten und gegebenenfalls den Umgang mit personenbezogenen Daten datenschutzrechtlich überprüfen.

## 5.11 Sichere mobile Kommunikation in der Bundesverwaltung

*Das BSI hat Sicherheitsstandards und Schutzprofile für die IT-Infrastrukturen in der Bundesverwaltung, insbesondere beim Einsatz mobiler Geräte entwickelt. Sie sollen die IT-Sicherheit gewährleisten und können auch zu einem besseren Datenschutz beitragen.*

Im beruflichen Einsatz ist die Kommunikation mittels mobiler Endgeräte, sogenannter Smartphones bzw. PDA, bereits gang und gäbe. Auch in der Bundesverwaltung wird – neben der SMS und der klassischen Telefonie – der mobile Zugriff auf E-Mails, den Terminkalender oder das Internet immer wichtiger, denn sie bringen für die Nutzer viele Vorteile.

Parallel zu der stärkeren Verbreitung der mobilen Datenkommunikation entstehen aber auch immer neue Bedrohungen für die IT-Sicherheit und den Datenschutz: Mobile Endgeräte sind lohnende Angriffsziele für Cyberkriminelle, die die teilweise unterentwickelten Sicherheitsstandards dieser Systeme ausnutzen. Zu den Gefahren gehören das Mitlesen der E-Mail-Kommunikation oder der Kurznachrichten, das Infizieren des mobilen Gerätes durch Schadsoftware oder die unerlaubte Nutzerortung (vgl. Nr. 6.2).

Ein vom BSI entwickeltes Schutzprofil soll den genannten Gefahren bei dem mobilen Datenaustausch begegnen. Dieses Schutzprofil beinhaltet das Konzept der durchgängigen Verschlüsselung sowie weitere integrierte Sicherheitsmassnahmen. Die Firma T-Systems verwendete das Schutzprofil bereits bei der Entwicklung des Systems SiMKo2 („Sichere Mobile Kommunikation“). Infolgedes-

sen empfiehlt das BSI den Einsatz dieses Geräts für Verschlusssachen mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“. Andere mobile Kommunikationslösungen werden nach dem derzeitigen Stand nicht empfohlen.

Auch für die mobile Sprachkommunikation ist der Schutz vor einem illegalen Zugriff durch Dritte unabdingbar. Da SiMKo2-Geräte derzeit noch kein verschlüsseltes Telefonieren unterstützen, eignen sie sich nicht für die mobile Sprachverbindung und den Austausch von Kurznachrichten, soweit es um klassifizierte Inhalte geht. Für diesen Zweck hat das BSI den Sicherheitsstandard „Sichere Netzübergreifende Sprachkommunikation“ (SNS) definiert. Die ersten mobilen Endgeräte nach SNS-Standard wurden bereits an die Bundesverwaltung ausgeliefert.

Mit der Zertifizierung der beiden Sicherheitsplattformen sind wichtige Voraussetzungen für eine sichere mobile Kommunikation innerhalb der Bundesverwaltung geschaffen worden.

### 5.12 Projekt D115 geht in den Regelbetrieb

*Nachdem ich bereits im letzten Tätigkeitsbericht ausführlich über das Projekt und den Pilotbetrieb berichtet hatte (vgl. 22. TB Nr. 2.7), wird derzeit unter Federführung des BMI der Regelbetrieb vorbereitet.*

Die im Feinkonzept für D115 festegelegten datenschutzrechtlichen Rahmenbedingungen haben sich im Pilotbetrieb weitgehend bewährt. Sie werden daher auch für den ab dem Jahr 2011 geplanten Regelbetrieb im Wesentlichen übernommen werden.

Die vorgesehene Organisationsstruktur des D115-Verbundes basiert auf einem Beschluss des IT-Planungsrates sowie einer Verwaltungsvereinbarung zwischen dem Bund und den bisher beteiligten Ländern. Die Einzelheiten sind in einer Geschäftsordnung und einer von den Teilnehmern des Verbundes zu unterzeichnenden Charta zu D115 festgelegt. Sowohl in der Verwaltungsvereinbarung als auch in der Charta ist die Einhaltung der gesetzlichen Anforderungen an Datenschutz und Datensicherheit für alle Projektteilnehmer ausdrücklich vorgegeben.

Damit ist auch klargestellt, dass die Regeln des allgemeinen Datenschutzrechts angewendet werden. Für den Umgang mit personenbezogenen Daten durch die auf Kommunal- und auf Landesebene betriebenen Servicecenter gilt das Landesdatenschutzgesetz des jeweiligen Landes. Für die teilnehmenden Behörden auf Bundesebene ist das Bundesdatenschutzgesetz anzuwenden. Es ist sichergestellt, dass spezifische landesrechtliche Anforderungen z. B. im Hinblick auf die Einwilligung zur Speicherung von Daten, die elektronische Weiterleitung von Anliegen oder die Löschungsfristen dieser Daten umgesetzt werden können.

Neu gegenüber dem Pilotbetrieb ist, dass für die elektronische Weiterleitung von Anliegen ein externer Dienstleister beauftragt werden soll, der die Nachrichten in Postfächer abspeichert, die vom empfangenden Teilnehmer abgerufen werden. Der Dienstleister kann nach meiner Auffassung nur im Wege der Auftragsdatenverarbeitung eingebunden werden. Verantwortliche Stelle ist jeweils der Träger desjenigen Servicecenters, das die Nachricht im Postfach zum Abruf durch den Empfänger abspeichert. Der Träger des Servicecenters (Kommune, Land oder Bund) muss für die Einhaltung der jeweils anwendbaren Bestimmungen zur Auftragsdatenverarbeitung (vgl. Nr. 2.4) sorgen.

### 5.13 Flugdrohnen – nur ein Spielzeug oder doch ein Spionage-Hubschrauber?

*Ferngesteuerte „Flugdrohnen“ werden seit einiger Zeit als Hightech-Spielzeug beworben. Die im Handel frei erhältlichen Minihubschrauber sind über eine spezielle Software per Smartphone steuerbar. Ein effektiver Rechtsschutz gegen Eingriffe in die Privatsphäre gestaltet sich schwierig. Das Datenschutzrecht stößt hier an seine Grenzen.*

Das Gerät wird von vier Propellern angetrieben und lässt sich über Software per Smartphone oder Tablet-PC steuern. Befehle werden per WLAN übermittelt, umgekehrt kann der Nutzer Live-Bilder der zwei Bordkameras auf dem Bildschirm seines Geräts ansehen.

Unbemannte Luftfahrzeuge haben in den letzten Jahren an Bedeutung zugenommen. Aufgrund ihrer vielfältigen Einsatzmöglichkeiten sind sie durch die Verordnung zur Änderung der Luftverkehrs-Ordnung und anderer Vorschriften des Luftverkehrs mittlerweile mit klarstellenden Regelungen in das sonstige Luftfahrtrecht integriert worden.

Eine aktuelle „Spielzeug“-Flugdrohne wiegt (nur) 400 g, kann bis zu 12 Minuten in der Luft bleiben und maximal 18 km/h fliegen, sie kann dabei eine Flughöhe von bis zu sechs Metern mit einer Reichweite von etwa 50 Metern erreichen. Eine Zulassung oder eine Aufstiegserlaubnis ist für Privatpersonen nicht erforderlich; Verkauf und Einsatz unterliegen keinerlei Beschränkung.

Es ist datenschutzrechtlich ohne Belang, wenn die Flugdrohne ausschließlich als flugtechnisches Geschicklichkeitsspiel verwendet wird – in öffentlich zugänglichen Bereichen. In öffentlich nicht zugänglichen Bereichen halte ich den Einsatz solcher Flugdrohnen wegen der Gefahren für die Privatsphäre für bedenklich, weil mit ihnen das Verhalten anderer Menschen heimlich beobachtet werden kann.

Wird die Drohne zum Ausspionieren bzw. für nicht erlaubtes Fotografieren/Filmen eingesetzt, bedeutet dies eine Verletzung der Privatsphäre und stellt ggf. einen Verstoß gegen das Datenschutzrecht dar. Soweit mit den Geräten Videoaufnahmen in der Öffentlichkeit gefertigt werden, ist § 6b BDSG einschlägig (vgl. Kasten zu Nr. 5.13). Im rein privaten Bereich gelten die Regelungen des Bundesdatenschutzgesetzes hingegen nicht – und darum wird es sich häufig handeln.

Die Betroffenen haben aber meist kaum eine Möglichkeit, sich gegen diesen Eingriff in ihre Privatsphäre effektiv zur Wehr zu setzen. Denn auch die den Betroffenen unter Umständen zustehenden zivilrechtlichen Unterlassungsansprüche setzen voraus, dass die Drohnen bemerkt

und einem konkreten Nutzer zugeordnet werden können. Schließlich ist die strafrechtliche Würdigung des Drohneneinsatzes – bei heimlichen Aufnahmen oder Übertragungen von Personen in Wohnungen und anderen geschützten Bereichen kann es sich um eine Straftat handeln (vgl. Kasten zu Nr. 5.13) – noch offen und erfolgt erst auf Grund eines Strafantrags des Betroffenen. Immerhin könnte im Falle einer Verurteilung die unzulässig verwendete Drohne gemäß § 74a StGB eingezogen werden.

Kasten zu Nr. 5.13

**§ 6b BDSG** (Auszug)

**Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen**

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

…

**§ 201a StGB** (Auszug)

**Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen**

(1) Wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

…

## 6 Telekommunikations- und Postdienstleistungen

### 6.1 Vorratsdatenspeicherung: Quo vadis?

*Nachdem das Bundesverfassungsgericht (BVerfG) die gesetzlichen Vorschriften zur Vorratsdatenspeicherung kassiert hat, stellt sich die Frage, wie es jetzt weiter geht. Die Antwort hängt auch von der Evaluierung der zugrunde liegenden europäischen Richtlinie ab.*

**Das Urteil des Bundesverfassungsgerichts**

In meinem 22. TB (Nr. 3.2.1) hatte ich die verfassungsrechtlichen Bedenken gegenüber der Vorratsdatenspeicherung (VDS) dargelegt und über die Verfassungsbeschwerde berichtet (für Hintergrundinformationen zur Vorratsdatenspeicherung vgl. Kasten a zu Nr. 6.1). Das BVerfG hat in seinem Urteil vom 2. März 2010 (1 BvR 256/08) die Verfassungswidrigkeit der Regelungen zur VDS festgestellt und diese für nichtig erklärt. Ich sehe das Urteil in einer Reihe mit den Grundsatzentscheidungen des BVerfG zur Volkszählung oder zur Online-Durchsuchung, die den Datenschutz in Deutschland gestärkt haben.

Dabei darf aber nicht übersehen werden, dass das Gericht lediglich die gesetzlichen Regelungen zur VDS als verfassungswidrig bewertete. Gleichzeitig äußerte es aber die Auffassung, dass die der VDS zugrunde liegende europäische Richtlinie durchaus verfassungskonform umgesetzt werden könne. Wegen der hohen Eingriffsintensität müsste die VDS jedoch besonders strengen Anforderungen unterliegen. Das Gericht nannte hier vier Kriterien:

- Hoher Standard der Datensicherheit,
- enge Grenzen der Datenverwendung,
- hinreichende Transparenz sowie
- effektiver Rechtsschutz.

Bei den Anforderungen an die Datensicherheit nahm das Gericht meine Forderungen auf. So müssen die Vorratsdaten von den sonstigen vom Unternehmen für betriebliche Zwecke genutzten Daten getrennt werden. Die Daten müssen verschlüsselt werden und einem gesicherten Zugriffsregime beim Provider unterliegen – beispielsweise durch ein Vier-Augen-Prinzip. Schließlich sind die Zugriffe auf die Daten revisionssicher zu protokollieren. Auch wenn sich bei der Einhaltung dieser Vorgaben Missbrauchsmöglichkeiten nicht vollständig auszuschließen lassen, könnte so die Gefahr des Missbrauchs zumindest stark reduziert werden.

Für besonders unzulänglich hielt das Gericht die gesetzlichen Regelungen zur Datenverwendung. So habe der Gesetzgeber versäumt, die Datenverwendung auf einen abschließenden Katalog schwerer Straftaten zu beschränken. Über diese eindeutig festzulegenden Strafverfolgungszwecke hinaus sei die Datenverwendung aufgrund ihrer hohen Eingriffsintensität nur zulässig, wenn dies für überragend wichtige Aufgaben des Rechtsgüterschutzes unerlässlich sei. Darüber hinaus beschränke sich das Gebot der restriktiven Datennutzung nicht nur auf die Anforderungen, unter denen die Daten an die Bedarfsträger übermittelt werden dürften, sondern es gelte auch für die Nutzung bereits übermittelter Daten. Diese dürften nur zweckgebunden verwendet werden und müssten schnellstmöglich verarbeitet und sofort gelöscht werden, wenn sie ihren Zweck erfüllt hätten.

Das Gericht stellte außerdem klar, dass die Datenerhebung und -nutzung grundsätzlich offen stattfinden müssen und nur ausnahmsweise im Einzelfall mit richterlicher Anordnung heimlich erfolgen dürfen. Durch ein effektives Rechtsschutzsystem müsse sichergestellt werden, dass die Datenübermittlung von den Telekommunikationsunternehmen an die Bedarfsträger grundsätzlich einem Richter-

vorbehalt unterliegt und die nachträgliche Kontrolle der Datenverwendung über ein effektives Rechtsschutzverfahren gesichert sei.

Hervorzuheben sind auch die Feststellungen des Gerichts, dass vorsorgliche, anlasslose Datensammlungen eine bestimmte Grenze nicht überschreiten dürfen (vgl. Kasten b zu Nr. 6.1.). Eine umfassende anlasslose Überwachung widerspräche der verfassungsrechtlichen Identität der Bundesrepublik Deutschland.

Positiv sehe ich die Feststellung der Verfassungsrichter, dass IP-Adressen dazu geeignet sein können, in weitem Umfang die Identität von Internetnutzern zu ermitteln. Allerdings seien für die Herausgabe von Kundendaten, deren Identität anhand der IP-Adressen festgestellt wurde, geringere Anforderungen zu stellen als für Auskünfte über sonstige Verkehrsdaten der Telekommunikation.

**Einfrieren als Alternative**

Auch wenn Telekommunikationsdaten in Deutschland nach dem Urteil des BVerfG nicht mehr auf Vorrat gespeichert werden dürfen, bedeutet dies nicht zwangsläufig ein endgültiges Aus für die Vorratsdatenspeicherung. Wie dargelegt, hat das Gericht zwar die gesetzliche Regelung für verfassungswidrig erklärt, gleichzeitig aber auch Hinweise für eine mögliche verfassungskonforme Umsetzung der VDS-Richtlinie gegeben. Angesichts dessen nimmt der Druck auf das hierfür zuständige Bundesministerium der Justiz (BMJ) zu, eine neue gesetzliche Regelung zur VDS vorzubereiten. Erfreulicherweise beugt man sich im BMJ diesem Druck bislang nicht.

Auch ich bin der Auffassung, dass eine voreilige Wiedereinführung der VDS falsch wäre. Zum einen ist m. E. der Nachweis nicht hinreichend erbracht worden, dass die Vorratsdatenspeicherung die Aufklärungsrate von schweren Straftaten tatsächlich in einem derartigen Maße verbessern würde, dass dies den mit ihr einhergehenden schwerwiegenden Eingriff in die Grundrechte sämtlicher Telekommunikationsnutzer rechtfertigen könnte. Offenbar ist der Mangel an empirischen Belegen kein rein deutsches Problem, denn die EU-Kommission hat den für 2010 vorgesehenen Evaluationsbericht zur VDS-Richtlinie mangels Zulieferung von aussagekräftigem Material aus den Mitgliedstaaten zunächst auf das erste Quartal 2011 verschoben (vgl. u.). Zum anderen erscheint es gleichwohl plausibel, dass bestimmte Straftaten, insbesondere solche, die ausschließlich über das Internet begangen werden, nur schwer aufzuklären sind, wenn die Zuordnung von dynamischen IP-Adressen zu Verursachern nicht möglich ist.

Ich bin deshalb dafür eingetreten, ein Verfahren zu suchen, das einerseits eine effektive Strafverfolgung ermöglicht, andererseits aber eine datenschutzfreundliche Alternative zur anlasslosen langfristigen Vorratsdatenspeicherung darstellt. Diese Anforderungen werden m. E. von einem modifizierten „Quick-Freeze“-Verfahren erfüllt, das ich bereits vor einiger Zeit in die öffentliche Diskussion eingebracht hatte.

Bei diesem Modell haben die Telekommunikationsanbieter auf Anordnung der Strafverfolgungsbehörden die Telekommunikationsdaten, die zur Aufklärung einer Straftat erforderlich sein können, von der Löschung auszunehmen, sie also für einen gewissen Zeitraum „einzufrieren“. Die Strafverfolgungsbehörden können in diesem Zeitraum dann einen richterlichen Beschluss erwirken, mit dem die Telekommunikationsunternehmen zur Herausgabe der Daten verpflichtet werden. Sollte ein solcher Beschluss nicht innerhalb einer gesetzlich vorgegebenen Zeit beigebracht werden können, werden die „eingefrorenen“ Daten gelöscht, ohne dass die Strafverfolgungsbehörden sie erhalten. Ein ähnliches Verfahren hat sich bei der Verfolgung von Urheberrechtsverletzungen durchaus bewährt (vgl. Nr. 4.8).

Problematisch wird dieses Konzept lediglich dort, wo Daten unmittelbar nach dem Verbindungsende gelöscht werden – etwa bei Internetzugangsdaten, die einem Flatratetarif unterfallen. Diese Daten müssten für einen gewissen kurzen Zeitraum von der regulären Löschung ausgenommen werden, um zum „Einfrieren“ überhaupt zur Verfügung zu stehen („Quick Freeze Plus“). Dies umzusetzen bedarf aber einer gezielten Evaluierung, inwieweit durch die sehr begrenzte Pufferung von Daten schwere Straftaten verhindert oder aufgeklärt werden können und welche Daten dafür im Einzelnen benötigt werden. Ich sehe es als eine Selbstverständlichkeit an, dass es sich hierbei um eine absolut restriktive Auswahl handeln muss und dass darüber hinaus die Daten besonderen Sicherheitsanforderungen – wie beispielsweise den vom BVerfG festgelegten Anforderungen zur Datensicherheit – unterliegen müssen.

Ich denke, dass ein solches Verfahren das öffentliche Interesse an der Verfolgung von Straftaten einerseits und den Schutz des Fernmeldegeheimnisses und des informationellen Selbstbestimmungsrechts andererseits auf einem für beide Seiten akzeptablen Niveau zum Ausgleich bringt.

**Eine neue Richtung aus Brüssel**

Noch ein weiterer Grund spricht gegen eine sehr frühzeitige Neuauflage eines Gesetzes zur VDS. Die Europäische Kommission führt zurzeit eine Evaluierung der VDS-Richtlinie durch und hat angekündigt, den ursprünglich für 2010 geplanten Evaluationsbericht bis zum Ende des ersten Quartals 2011 vorzulegen. Auch wenn nach gegenwärtigem Stand eine vollständige Aufhebung der Richtlinie – wie sie auch in einer Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (vgl. Kasten c zu Nr. 6.1) gefordert wurde – als unwahrscheinlich gilt, gibt es Signale der Kommission, dass es jedenfalls Änderungen der Vorschriften geben könnte. So unterstützt die für das Datenschutzrecht zuständige EU-Kommissarin Redding das von mir vorgeschlagene Verfahren Quick Freeze Plus als sinnvolle Alternative zur anlasslosen VDS. Zudem hat die für die VDS-Richtlinie zuständige Innenkommissarin Malmström kürzlich in einer Rede angedeutet, dass die Tendenz der Kommission dahin gehe, die Richtlinie insbesondere im Hinblick auf die Datenverwendung klarer zu gestalten und dabei auch die Dauer der Speicherfristen zu verkürzen.

Der Entscheidung der Kommission geht das bereits angesprochene Evaluierungsverfahren voraus, an dem auch ich mich beteiligt habe. So habe ich im Rahmen einer Untersuchung der Artikel-29-Gruppe im Jahr 2009 Kontrollen bei mehreren Telekommunikationsunternehmen durchgeführt, um mir auch von der praktischen Umsetzung der Vorratsdatenspeicherung ein besseres Bild machen zu können. Die dabei gewonnenen Erkenntnisse – die auch erhebliche Umsetzungsdefizite betreffen – sind sowohl in meine Stellungnahmen gegenüber dem BVerfG als auch in einen Bericht der Artikel-29-Gruppe (WP 172 vom 13. Juli 2010) eingegangen, der der Kommission im Rahmen des Evaluierungsverfahren zur Verfügung gestellt wurde.

Kasten a zu Nr. 6.1

**Hintergrundinformationen zur Vorratsdatenspeicherung**

Am 15. März 2006 wurde die EG-Richtlinie 2006/24/EG beschlossen, mit der den Mitgliedstaaten europaweit die Einführung einer Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten zur Verfolgung schwerer Straftaten auferlegt wurde (vgl. 21. TB Nr. 10.1). In Deutschland wurde diese Richtlinie mit dem „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ am 1. Januar 2008 in nationales Recht umgesetzt. Aufgrund dieser Gesetzesänderung wurden Telekommunikationsunternehmen verpflichtet, die Verkehrsdaten ihrer Kunden über einen Zeitraum von sechs Monaten zu speichern und bei Bedarf den Strafverfolgungsbehörden, den Polizeibehörden für präventiv-hoheitliche Aufgaben sowie den Nachrichtendiensten zur Verfügung zu stellen, soweit diese über eine entsprechende gesetzliche Auskunftsbefugnis verfügen.

Bei den zu speichernden Daten handelte es sich unter anderem um Telefonverbindungsdaten wie die Rufnummer des Anrufers und des Angerufenen, den genauen Zeitpunkt und die Dauer eines Gespräches sowie bei Mobilfunkgesprächen die Funkzelle, in der das Gespräch begonnen wurde, und die eindeutige SIM-Karten- und Handy-Identifikationsnummer. Ab dem 1. Januar 2009 wurde die Speicherpflicht auch auf solche Daten erweitert, die bei der E-Mail- und Internet-Nutzung anfallen. In diesem Zusammenhang sind insbesondere die IP- und E-Mail-Adresse zu nennen.

Mit Urteil vom 2. März 2010 erklärte das BVerfG die gesetzlichen Vorschriften zur Vorratsdatenspeicherung für verfassungswidrig und nichtig. Neben dem deutschen hat auch das rumänische Verfassungsgericht die nationale Umsetzung der Richtlinie zur Vorratsdatenspeicherung für verfassungswidrig erklärt. Ein vergleichbares Verfahren ist auch beim ungarischen Verfassungsgericht anhängig. Der irische High-Court hat darüber hinaus dem Europäischen Gerichtshof (EuGH) die Frage vorgelegt, ob die Richtlinie mit den verbrieften Grundrechten der Gemeinschaft vereinbar ist. Der EuGH hatte Anfang des Jahres 2009 festgestellt, dass die Richtlinie formell auf der richtigen Rechtsgrundlage erlassen wurde. Ausführungen zur inhaltlichen Rechtmäßigkeit blieben bei der damaligen Prüfung aber explizit unberücksichtigt.

Vor einer Entscheidung durch den EuGH könnte die Richtlinie aber bereits durch die Kommission abgeändert werden. Ein entsprechendes Evaluierungsverfahren soll voraussichtlich zum Ende des ersten Quartals 2011 abgeschlossen sein.

Kasten b zu Nr. 6.1

**Zitate aus dem Urteil des BVerfG zur Vorratsdatenspeicherung**

„Eine Speicherung kann nicht als solche abstrakt gerechtfertigt werden, sondern nur insoweit, als sie hinreichend gewichtigen, konkret benannten Zielen dient.“

„Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung [...] setzt voraus, dass diese eine Ausnahme bleibt. Sie darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen.“

„Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss.“

Kasten c zu Nr. 6.1

**Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010**

**Keine Vorratsdatenspeicherung!**

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt". Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale ELENA-Datenbank muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

## 6.2 Denn sie wissen, wo Du bist – Ortungsdienste im Wandel

*Immer mehr mobile Geräte ermöglichen eine immer genauere Feststellung, wo sich deren Besitzer aufhalten.*

Mobiltelefone und andere mobile Endgeräte können nur genutzt werden, wenn sie mit Funknetzen verbunden sind. Auf diese Weise entstehen – als Nebenprodukt – Standortdaten, die zumindest den Netzbetreibern bekannt sind. Allerdings sind diese Daten auch für sonstige Dritte von Interesse: Für Anbieter von „Location Based Services", aber auch für Werbetreibende und Notdienste.

Die in immer mehr mobile Geräte eingebauten Techniken zur Selbstortung mittels Satellit und die Verwendung der Kenndaten von WLAN-Netzen (vgl. Nr. 4.1.2) gestatten eine fast metergenaue Ortung – selbst in geschlossenen Räumen. Je genauer die Standortdaten sind, desto interessanter sind sie für mögliche Nutzer und desto bedeutsamer wird der Schutz der Betroffenen vor heimlicher Ortung. Auch wenn es jeweils um die Feststellung des Standorts von mobilen Geräten geht, ist die rechtliche Würdigung von Ortungsmechanismen kompliziert – Grund genug für ein Update meiner bisherigen Berichterstattung zu diesem Thema (vgl. zuletzt 22. TB Nr. 7.7).

### Handyortung nach dem Telekommunikationsgesetz (TKG)

In meinem 22. TB hatte ich bereits über einen Gesetzentwurf zur Änderung des TKG berichtet, der schließlich im August 2009 Gesetzeskraft erlangte (BGBl. I S. 2409). Hiermit sollte für die klassische Mobilfunkortung, die von den Netzbetreibern durchgeführt wird, der Missbrauchsgefahr entgegengewirkt werden. Die wichtigsten Neuerungen waren, dass für Ortungen durch Dritte eine schriftliche Einwilligung des Teilnehmers gefordert wird und dass nach fünf Ortungen eine Informations-SMS an diesen verschickt werden muss.

Bei der Umsetzung der gesetzlichen Vorgaben zeigten sich jedoch Unklarheiten und Umgehungsmöglichkeiten. So wird nicht zweifelsfrei geregelt, wer wofür verantwortlich ist. Der Handyvertrag kann bei einem Serviceprovider abgeschlossen worden sein, der Mobilfunkdienst wird vom Netzbetreiber erbracht, ein Ortungsanbieter betreibt die Ortungsplattform und schließt die Verträge zur Ortung ab. Nur der Serviceprovider kennt den Teilnehmer, hat aber mit dem eigentlichen Ortungsvorgang nichts zu tun.

Die Bundesnetzagentur (BNetzA) sieht nicht zuletzt aus Gründen der Praktikabilität den Ortungsanbieter als Verpflichteten zur Entgegennahme der schriftlichen Einwilligung. Um dem Missbrauchsrisiko zu begegnen, habe der Ortungsdiensteanbieter allerdings geeignete Maßnahmen zur Sicherstellung einer wirksamen Einwilligung zu treffen. Maßnahmen dieser Art könnten darin liegen, dass zusammen mit der Einwilligung eine Erklärung des Teilnehmers eingeholt wird, in der dieser versichert, Vertragspartner zu der angegebenen Mobilfunkrufnummer zu sein.

Ich habe Zweifel, dass hiermit dem Missbrauch effektiv begegnet wird. Die im TKG vorgesehene Informations-SMS – theoretisch vom Serviceprovider zu versenden, der nichts von der Ortung weiß – greift nur, wenn kein Widerspruch gegen die SMS-Benachrichtigung eingelegt wurde. Die im Gesetz vorgesehene Möglichkeit zum Verzicht auf Benachrichtigung dürfte einen Missbrauch in manchen Fällen erst ermöglichen.

Ein weiteres Problem ist die Eigenortung. Ein Teilnehmer, also der Kunde, der sein eigenes Handy orten will, muss weder entsprechend § 98 TKG schriftlich einwilligen noch braucht er eine Informations-SMS zu erhalten. Eine „gesetzeskonforme" Eigenortung in diesem Sinne wäre auch dann gegeben, wenn der Teilnehmer mehrere SIM-Karten besitzt, etwa eine Partnerkarte für seinen Ehepartner oder bei auf einen Arbeitgeber gebuchten Diensthandys, die er seinen Mitarbeitern auch zur priva-

ten Nutzung zur Verfügung stellt. In diesen Fällen liegt aber gar keine wirkliche Eigenortung vor, sondern der Mechanismus wird verwendet, um den Aufenthaltsort einer anderen Person festzustellen. Hier würden sowohl das Schriftformerfordernis für die Einwilligung als auch die Benachrichtigungs-SMS entfallen und somit ein Missbrauch erleichtert.

Angesichts dieser Risiken begrüße ich es, dass viele Anbieter unabhängig von der jeweiligen Fallkonstellation stets eine Einwilligungs-SMS verlangen, die vom zu ortenden Handy verschickt werden muss, ehe die Ortung freigeschaltet wird.

Das BMWi hat auf diese Probleme reagiert und im Rahmen der aktuellen TKG-Novelle auch § 98 TKG zur Diskussion gestellt. In der zum Redaktionsschluss vorliegenden Fassung soll – auf meinen Vorschlag hin – eine Informations-SMS immer, also ohne Widerspruchsmöglichkeit, an das Endgerät gesendet werden, es sei denn, dass die Standortdaten nur am Endgerät angezeigt werden. Eine solche Eigenortung würde etwa bei einem Dienst zur Anzeige der Restaurants in der Umgebung vorliegen. Ich hoffe, dass die vorgeschlagene Regelung möglichst bald beschlossen wird, um die Missbrauchsrisiken bei Ortungsdiensten zu verringern.

**Ortung von Smartphones**

Während die Ortung über die Mobilfunk-Netzbetreiber mit jedem Handy möglich ist, aber selten genutzt wird, wird die Standortbestimmung von Smartphones zur alltäglichen Routine. Inzwischen gehört der Besitz eines solchen Klein-Computers mit Telefon-, Foto-, WLAN- und GPS-Ortungs-Funktion sowie einer Daten-Flatrate in manchen Kreisen schon fast zum guten Ton (vgl. auch Nr. 5.11). Dabei erfolgt die Ortung mit Hilfe von GPS-, WLAN- und Mobilfunkdaten ohne Beteiligung des Mobilfunk-Netzbetreibers. Die per Funk empfangenen Daten werden in der Regel an einen – meist amerikanischen – Anbieter über das Internet übermittelt, der den Standort bestimmt. Neben den GPS-Daten werden auch Datenbanken mit Messwerten von WLAN-Stationen und Mobilfunksendern verwendet, so dass auch ohne GPS-Empfang eine Standortbestimmung möglich ist. Umgekehrt bilden die vom Smartphone übertragenen Daten – zusammen mit Daten von Messfahrten (vgl. Nr. 4.1) – die hierfür notwendige Datenbasis. Somit kann man z. B.

- sich eine Straßenkarte der Umgebung anzeigen lassen,
- ein Foto mit einem „Geo-Tag“ versehen lassen,
- den eigenen Standort den Freunden in einem sozialen Netzwerk bekannt geben
- oder Werbung mit Ortsbezug erhalten.

Diese Standortdaten unterliegen nicht dem TKG, sondern dem Telemediengesetz, da der Telekommunikationsanbieter die Ortung nicht selbst durchführt. Somit sind die Datenschutzaufsichtsbehörden der Länder zuständig. Da in vielen Fällen amerikanische Unternehmen den Dienst anbieten, haben europäische Aufsichtsbehörden leider nur wenig Einfluss auf die Erhebung und Verwendung der Standortdaten.

Die wenigsten Nutzerinnen und Nutzer verstehen, welche Prozesse ablaufen, wenn sie über ein Smartphone nach Restaurants in der näheren Umgebung suchen. Überraschend waren die Einzelheiten in der Stellungnahme eines amerikanischen Unternehmens vom Sommer 2010 an den US-Kongress zu den Ortungsfunktionen seiner Geräte. Darin wird erläutert, dass die Endgeräte bei aktivierter Ortung pseudonymisierte Messdaten an das Unternehmen senden oder dass – sofern kein Widerspruch gegen ortsbezogene Werbung erfolgte und die Ortungsfunktion nicht deaktiviert ist – der Aufenthaltsort mit der Genauigkeit von Postleitzahlen (ZIP-Code) personenbezogen gespeichert wird. Es gibt auch Vorgaben für Hersteller von Anwendungen, die ein Kunde auf das Gerät laden kann, etwa dass der Kunde eingewilligt haben muss und die Ortsinformation für die Anwendung erforderlich ist. Selbst wenn einige Punkte geklärt werden, bleiben bei genauerer Betrachtung der Stellungnahme noch viele Fragen wie z. B. die Speicherdauer von Daten offen. Auch kann man unterschiedlicher Meinung sein, ob Daten anonym, pseudonym oder personenbeziehbar sind.

Diese Datenübermittlungen finden im Allgemeinen erst nach einer Einwilligung in die Nutzungsbedingungen statt. Fraglich dürfte auch sein, ob die wenigen, die diese überhaupt lesen, die ganze Tragweite verstehen. Hier muss ich an jeden Nutzer appellieren, sich vor einer Einwilligung bzw. Freischaltung der Ortungsfunktion den möglichen Umfang zu vergegenwärtigen und ein gesundes Misstrauen walten zu lassen.

**Notrufortung**

Nachdem die Notrufverordnung am 6. März 2009 erlassen worden ist (BGBl. I S. 481), erwarte ich die Technische Richtlinie Notrufverbindungen (TR Notruf) für Anfang 2011. Ein erster Entwurf enthielt keine Lösung für die von mir problematisierten Punkte. Insbesondere soll für die Standortbestimmung in Fällen, bei denen mehrere Netzbetreiber beteiligt sind, etwa VoIP-Anbieter und Internetanbieter, eine Mitwirkungspflicht eingeführt werden. In der Notrufverordnung wird darauf hingewiesen, dass die technischen Schnittstellen durch angemessene Maßnahmen gegen Missbrauch zu sichern sind. In dem Entwurf zur TR Notruf ist jedoch kein Hinweis zur konkreten Umsetzung enthalten. Eine zufriedenstellende technische Lösung hierfür ist für mich noch nicht absehbar. Da eine Ortsbestimmung bei VoIP bereits für die Feststellung der zuständigen Notrufabfragestelle notwendig ist, muss eine Lösung gefunden werden, bei der ein Nutzer einer IP-Adresse nicht durch Missbrauch der für Notruf standardisierten Schnittstellen von Nichtberechtigten lokalisiert werden kann.

Die Standortübermittlung von Mobilfunkteilnehmern an Notrufabfragestellen soll nach der TR Notruf nunmehr klarer geregelt werden. Bisher kann bei Bedarf der Standort eines Mobilfunkteilnehmers über die ursprünglich von der Björn-Steiger-Stiftung initiierte Notrufortung festgestellt werden, die inzwischen von der Allianz OrtungsServices GmbH (AOS) betrieben wird. Dabei wurde von der Notrufabfragestelle bisher eine mündliche Einwilligung

im Einzelfall eingeholt. Aufgrund der Änderung von § 98 TKG wäre nun eine schriftliche Einwilligung erforderlich – bei Notfällen wenig praktikabel. Deshalb wurde vorgeschlagen, eine Ortung formal nach § 108 TKG durchzuführen, wobei die AOS als Auftragsdatenverarbeiter für die Netzbetreiber tätig wird. Somit wäre der Form Genüge getan, dass die Standortdaten des Anrufers vom Netzbetreiber an die Notrufabfragestelle übermittelt werden. Bis zur verpflichtenden Anwendung der TR Notruf wäre dies eine gesetzeskonforme Lösung. Zum Zeitpunkt des Redaktionsschlusses waren aber noch nicht alle hierfür erforderlichen Verträge unterzeichnet.

### 6.3 Erfahrungen aus Kontrollen – unentbehrlich für die tägliche Arbeit

*Die Verarbeitung von Bestands- und Verkehrsdaten ist im Telekommunikationsgesetz geregelt. In der Praxis zeigt sich, dass Unternehmen bisweilen die Auslegungsspielräume dieser Vorschriften überschreiten.*

Ein Telekommunikationsanbieter hatte sich an mich gewandt, da er Zweifel an der Rechtmäßigkeit der eigenen Datenverarbeitung hatte. Einer der eklatantesten Punkte betraf die Löschung der Bestandsdaten ehemaliger Kunden. Diese Daten müssen mit Ablauf des auf die Vertragsbeendigung folgenden Jahres gelöscht bzw. – soweit aus steuer- und handelsrechtlichen Gründen noch Aufbewahrungspflichten bestehen – gesperrt werden; spätestens nach zehn Jahren gibt es keinen Grund für eine Speicherung.

Beim Systemdesign hatte man solche Kleinigkeiten offenbar außer Acht gelassen und für verschiedene Zwecke diverse Datenbanken kreuz und quer verbunden. Als nun eine Löschung bzw. Sperrung umgesetzt werden sollte, stellte man fest, dass die Daten in vielen Systemen gespeichert wurden und wie komplex deren Vernetzung war. Die gesetzlich notwendigen Systemänderungen erfordern einen erheblichen Aufwand. Auch bei der Verarbeitung der Verkehrsdaten waren Probleme erkennbar, etwa die Speicherung von Daten über netzinterne Gespräche, für die es bei Kunden mit Flatrate keinerlei Grund gibt, oder die zu lange Speicherung von Rohdaten aus den Vermittlungsstellen.

Ich habe trotz dieser Mängel von einer förmlichen Beanstandung abgesehen, da mich der Anbieter auf eigene Initiative auf seine Unzulänglichkeiten aufmerksam gemacht und bereits eigenständig umfangreiche Maßnahmen zu deren Abstellung ergriffen hat. Im Rahmen einer Kontrolle, die noch nicht abgeschlossen ist, begleite ich diesen Vorgang aufmerksam.

In meinem letzten Tätigkeitsbericht (Nr. 3.2.2) hatte ich bereits ausführlich über meine Prüfungen bei der Deutschen Telekom AG (DTAG) im Festnetz berichtet, die ich aus Anlass des „Telekom-Skandals“ durchgeführt hatte. Im genannten Beitrag hatte ich auch bereits über die Beanstandung informiert, die formal erst Anfang 2009 ausgesprochen wurde. Beanstandet hatte ich insbesondere, dass der Konzerndatenschutz keinen vollständigen und ausreichend detaillierten Überblick über die Datenverarbeitungssysteme hatte. Das Unternehmen hat zwischenzeitlich verschiedene Maßnahmen umgesetzt, die bereits eine deutliche Verbesserung bewirkt haben. Bei einem Konzern dieser Größe scheinen strukturelle Veränderungen jedoch eine recht langfristige Aufgabe zu sein.

Auch bei der Verarbeitung personenbezogener Daten wurden inzwischen Fortschritte erzielt. So werden Verkehrsdaten, die aufgrund einer Flatrate nicht abrechnungsrelevant sind, früher gelöscht. Die Anzahl der Nutzer einer Anwendung, mit der nur in besonderen Fällen auf Verkehrsdaten zugegriffen wird, wurde reduziert. Die Speicherdauer bei einem Verfahren zur Missbrauchserkennung wurde deutlich herabgesetzt. Für den Festnetzbereich habe ich zum Ende des Berichtszeitraums bei der Speicherung von Verkehrsdaten für die Abrechnung mit anderen Netzbetreibern (Intercarrierabrechnung) einen Dissens mit dem Unternehmen. Dieser bezieht sich auf die Interpretation des im Datenschutzrecht wichtigen Begriffs *„erforderlich“*. Nach der gesetzlichen Vorgabe im TKG dürfen Verkehrsdaten verarbeitet werden, soweit dies für betriebliche Zwecke, also die Erbringung eines Dienstes oder seine Abrechnung erforderlich ist.

Es ist ein generelles Problem, dass der Übergang zwischen *(zwingend) erforderlich* und *ganz praktisch (für alle Eventualitäten)* oft fließend ist und von manchen Unternehmen eher zu ihren Gunsten ausgelegt wird. Dies zeigt sich etwa bei der Speicherung der Daten zur Missbrauchserkennung gemäß § 100 Absatz 3 TKG, die nur bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte und damit nur in sehr engen Grenzen zulässig ist. Mit der zunehmenden Verbreitung von Flatrates werden in Bezug auf den Endkunden weniger Daten aus betrieblichen Gründen erforderlich – umso problematischer sehe ich es, wenn für die Abrechnung mit dem Kunden nicht mehr erforderliche Verkehrsdaten zu anderen Zwecken, insbesondere zur Missbrauchserkennung und -bekämpfung, vorgehalten werden. Auch geschäftliche Interessen rechtfertigen keine anlasslose Vorratsdatenspeicherung!

Bei der DTAG habe ich ebenfalls den Bereich Mobilfunk geprüft. Auch hier war es sehr mühsam, einen Überblick über die Verarbeitung der Verkehrsdaten zu erlangen, was meine bereits für den Festnetzbereich geäußerte Kritik nachträglich bestätigt. Die oben genannten Maßnahmen waren zum Zeitpunkt der Kontrolle im Mobilfunkbereich noch nicht realisiert.

Meine Kritik bezieht sich auf verschiedene Aspekte der Datenverarbeitung: Die Speicherung von Rohdaten aus den Vermittlungen war deutlich zu lange. Diese Daten werden für den Fall gespeichert, dass es technische Probleme bei den nachfolgenden Systemen zur Berechnung des Entgelts gibt und die Rohdaten nochmals die Verarbeitungskette durchlaufen müssen. Technische, vom Unternehmen zu verantwortende Probleme rechtfertigen – bei allem Verständnis für die Interessen an der Abrechnung von Entgelten – keine Verstöße gegen die gesetzlichen Vorgaben. Das TKG schreibt vor, dass die für die Berechnung der Entgelte erforderlichen Daten unverzüglich zu ermitteln und andere Daten unverzüglich zu löschen sind. „Unverzüglich“ bedeutet zwar nicht sofort, aber eine über

mehr als sieben Tage andauernde Speicherung solcher Daten halte ich generell nicht für vertretbar. Die DTAG muss ihre Verarbeitungsprozesse so optimieren, dass die gesetzlichen Vorgaben eingehalten werden.

Kritisch sehe ich auch den Umgang mit Verkehrs- und Nutzungsdaten bei einem im Aufbau befindlichen System für den Kundenservice. Auch wenn ich das Argument nachvollziehen kann, dass durch die immer komplexeren Dienste der Mobilfunkanbieter manche Fehlerquellen nur schwer zu analysieren sind, rechtfertigt dies keine exzessive Datenspeicherung. Der Umfang der – insbesondere entsprechend der anfänglichen Planung – gespeicherten Daten erscheint mir unverhältnismäßig.

Die vorgenannten Beispiele belegen, dass ich bei Beratungs- und Kontrollbesuchen oft auf Sachverhalte aufmerksam werde, die anhand gesetzlicher Vorgaben schwierig zu beurteilen sind. Nur vor Ort ist zu erkennen, ob die gesetzlichen Anforderungen umgesetzt werden. All dies zeigt, wie wichtig diese Kontrollen sind, die jedoch einen hohen personellen Aufwand bedeuten, angefangen von der Vorbereitung des Besuchs über den Kontrollbericht bis hin zur Prüfung der Umsetzung.

Bei dieser Gelegenheit möchte ich auch anmerken, dass das hinhaltende Verhalten mancher TK-Anbieter ebenfalls nicht unerhebliche personelle Ressourcen bindet und meine Arbeit unnötig erschwert. Mancher Vorgang – sowohl bei Kontrollen als auch bei Bürgereingaben – besteht aus fast ebenso vielen Erinnerungsschreiben wie aus produktivem Schriftverkehr. Ich werde Verstöße gegen die gesetzliche Kooperationspflicht mit dem BfDI zukünftig ggf. beanstanden. Leider habe ich – anders als die Aufsichtsbehörden der Länder – nicht die Möglichkeit, derartige Verstöße mit einem Bußgeld zu belegen (vgl. Nr. 2.1).

### 6.4 Kein Anschluss unter dieser URL – Tippfehler als Geschäftsmodell

*Ob es sich hier um eine praktische Hilfe bei Vertippern oder – wie eine Computerzeitschrift meinte – um einen Lausbubenstreich handelt, ist umstritten. In jedem Fall ist für den offensichtlich einträglichen Dienst eine Einwilligung des Kunden erforderlich.*

Ein Vertippen in der Adress-Zeile eines Browsers, etwa ein wwww.bfdi.bund.de, hatte bisher die Fehlermeldung „Error 404“ des abgefragten DNS-Servers zur Folge. Damit wusste der Internetnutzer, dass die Adresse so nicht existiert und konnte sie korrigieren. Noch bequemer mag ein neuer Service der Internetanbieter sein. Statt der Fehlermeldung wird eine Suchmaschine bemüht, um zu erraten, was der Nutzer meinte. Das Ergebnis wird dem Nutzer angezeigt – natürlich verbunden mit Werbung. Ob man dies als praktisch empfindet, ist Ansichtssache. Nicht immer ist das Gesuchte dabei und im heimischen Computernetz können die Seitenumleitungen zunächst unerklärliche Reaktionen auslösen, da sich einige Programme auf die übliche Fehlermeldung des DNS-Servers verlassen.

Aufgrund einiger Eingaben habe ich die Thematik näher betrachtet. Die DNS-Abfrage (vgl. Kasten zu Nr. 6.4) ist – rechtlich betrachtet – Teil des Telekommunikationsdienstes „Internetzugang“, mit der Folge, dass das Fernmeldegeheimnis greift. Das Angebot von Inhalten durch eine Suchmaschine ist demgegenüber ein Telemedienangebot. Daten, die dem Fernmeldegeheimnis unterliegen, dürfen nur dann für andere Zwecke – hier Umleitung einer angeforderten URL auf eine Suchseite – genutzt werden, wenn der Teilnehmer eingewilligt hat. Schließlich handelt es sich um einen grundsätzlich anderen Dienst, der für den Internetzugang selbst nicht erforderlich ist. Zudem erfährt der Anbieter der Suchmaschine, für welche Inhalte sich der Nutzer interessiert, ohne dass dieser den Dienst dieses Anbieters überhaupt in Anspruch nehmen wollte. Wer diese Argumentation nicht als ausreichend stichhaltig empfindet, mag sich das Zugangserschwerungsgesetz (vgl. hierzu Nr. 4.6) ansehen. In § 11 ZugErschwG wird bei technisch ähnlicher Vorgehensweise explizit festgestellt, dass das Fernmeldegeheimnis eingeschränkt wird, wenn eine URL-Anforderung etwa auf ein virtuelles „Stoppschild“ umgelenkt wird. Nutzt jemand hingegen eine Suchmaschine direkt, um die gewünschte Website zu finden – ggf. auch mit Schreibfehler –, ist dies ein direkter Kommunikationsvorgang zwischen dem Nutzer und dem Suchmaschinenanbieter: Der Nutzer erhält Seitenvorschläge mit vermeintlich richtigen Angaben. Dies ist rechtlich nicht zu beanstanden, weil für den Betreiber einer Suchmaschine das Fernmeldegeheimnis nicht gilt.

Die Netzbetreiber waren zunächst nicht von der Notwendigkeit zu überzeugen, dass eine Einwilligung erforderlich ist. Ob dies daran lag, dass man einen von manchen Kunden als bequem empfundenen Dienst erhalten wollte, oder daran, dass bei den präsentierten Vorschlägen auch bezahlte Verweise auf kommerzielle Internetangebote enthalten waren, möchte ich hier nicht kommentieren. Einige Anbieter wollen nun nach einem Vertipper die Einwilligung beim Nutzer einholen. Somit kann dieser Kunde künftig die Suchseite erhalten. Ebenso soll es möglich sein, dass ein Kunde auf Wunsch die klassische Fehlermeldung erhält. Diese Vorgehensweise entspricht sowohl dem Fernmeldegeheimnis als auch dem Interesse der Netzbetreiber und mancher Kunden.

Kasten zu Nr. 6.4

Das **Domain Name System (DNS)** dient zur Namensauflösung im Internet, um die logischen Namen von über das Internet abfragbaren Ressourcen in maschinenauswertbare IP-Adressen umzuwandeln. Wenn man im Web-Browser eine URL (Uniform Resource Locator) eingibt, fragt der PC beim DNS-Server des Routers nach, der wiederum den DNS-Server des Internet-Providers befragt. Von diesem erhält der PC mittels Router die IP-Adresse des Servers, auf dem die abgefragte Website gespeichert ist. Um die Website abzufragen, schickt der PC eine Anfrage an die so ermittelte IP-Adresse des

Web-Servers. Dieser Server schickt dann die Antwort an den PC, der die Inhalte anzeigen kann. Auch bei anderen Diensten, etwa beim Mailversand, wird die logische Adresse (etwa „bfdi.bund.de“ in poststelle@bfdi.bund.de) über das DNS-System in die IP-Adresse des Mailservers umgewandelt.

## 6.5 Deep Packet Inspection: Dürfen Anbieter Kommunikationsinhalte durchsehen?

*Anbieter von Telekommunikationsdiensten dürfen Kommunikationsinhalte nur ausnahmsweise zur Störungsbeseitigung durchsehen. Die Auswertung von Inhaltsdaten mittels Deep Packet Inspection und deren Speicherung in Log-Dateien bei Proxy-Servern ist unzulässig.*

Durch die Kontrolle eines Mobilfunkanbieters stellte ich fest, dass bei der mobilen Internetnutzung eine Anpassung der Daten (Internetseiten) vorgenommen und zusätzlich die Anpassung innerhalb einer Log-Datei dokumentiert wird. Hierbei wurde die von einem Proxy-Server (vgl. Kasten a zu Nr. 6.5) umgesetzte Anpassung der Inhalte genutzt, um zusätzlich zu den Kopfdaten weitere Informationen aus dem Inhalt der Datenpakete innerhalb der Log-Dateien zu speichern. Eine ähnliche Vorgehensweise ist auch unter Verwendung der Deep Packet Inspection (vgl. Kasten a zu Nr. 6.5) möglich, welche zum Teil bei den Netzbetreibern verfügbar ist.

Die Anbieter berufen sich vornehmlich auf § 100 Absatz 1 TKG, wonach sie Bestands- und Verkehrsdaten der Nutzer zum Zwecke der Störungsbeseitigung erheben und verwenden dürfen. Die aufgezeichneten Daten umfassen zusätzlich zu den üblichen Verkehrsleitinformationen auch die vom Nutzer „angesurfte“ URL, den in der Antwort enthaltenen HTML-Statuscode sowie den Browsertyp und werden (teilweise) anonymisiert vorgehalten. Die URL wird vor der Verarbeitung der Informationen auf den Domainnamen reduziert. Somit ist denkbar, dass die aufgezeichneten Daten nicht nur zur Störungsbeseitigung, sondern auch zur weiteren – im Regelfall statistischen – Auswertung des Nutzungsverhaltens verwendet werden, etwa für Verkehrsmessungen des mobilen Internetzugangs. Darüber hinaus eignen sich die gesammelten Informationen auch zur Auswertung der Besuchsfrequenz einer bestimmten Internetseite und für Erstellung und/oder Bewertung von Marketingkonzepten. Bei der genaueren Betrachtung dieser Technologie und ihres Einsatzes stellt sich die Frage, ob die Analyse der Pakete mit dem Fernmeldegeheimnis vereinbar ist, von der Frage der Regulierung von Datenströmen ganz abgesehen.

Der Zugang zum und die Datenübertragung im Internet ist heute, aus technischer Sicht, als digitale Paketkommunikation ausgelegt. Hierbei werden die zu übertragenden Daten (z. B. Internetseiten, E-Mails etc.) in kleine „Teile“ zerlegt, in Pakete verpackt und über Datenleitungen zwischen den verschiedenen Routern im Internet übertragen, bis sie schließlich vom Provider z. B. über den DSL-Anschluss an den heimischen Computer gesendet werden oder per Mobilfunk auf z. B. dem Smartphone ankommen. Generell wird bei Paketen eine Unterteilung in Nachrichtenkopf (im Allgemeinen als Header bezeichnet) und Datenanteil vorgenommen. Der Header beinhaltet die für die Wegeleitung und technische Verarbeitung der Datenpakete notwendigen Informationen. Die Kopfdaten von Paketen sowie deren Inhalt variieren mit dem jeweilig verwendeten Protokoll sehr stark; es ist nicht unüblich, dass unterschiedliche Protokolle ineinander verschachtelt als hierarchische Datenstruktur verwendet werden (vgl. Kasten b zu Nr. 6.5). Dieser Aufbau führt zu einer mitunter großen Ansammlung von Daten, von denen nur ein geringer Anteil zur technischen Verarbeitung beim Zugangsanbieter notwendig ist. Im Unterschied zur klassischen Telefonie werden Datenpakete (in der Regel) ohne eine direkte Verbindung zum Ziel (verbindungslos) übertragen. Wo beim Telefongespräch die Telefonnummer das Ziel bestimmt und einen eigenen Kommunikationskanal ermöglicht, müssen Datenpakete permanent anhand ihrer Kopfdaten analysiert und im Internet weitergesendet werden. Damit wird zunehmend die Unterscheidung eines einzelnen Datums und seine Qualifizierung als Verkehrs-, Nutzungs- oder Inhaltsdatum schwierig (vgl. 22. TB Kasten zu Nr. 7.8).

Während über die Qualifizierung der Telefonnummer einer angeforderten Verbindung als Verkehrsdatum kein Zweifel besteht, ist die Zuordnung einer in einem verschachtelten Protokoll enthaltenen URL (einer angeforderten Internetseite) zu einer Datenkategorie dagegen strittig. Hierbei ist eine Betrachtung des Anwendungsfalls unerlässlich. Wenn z. B. ein Server mehrere Internetseiten beherbergt, aber nur mit einer IP-Adresse ausgestattet ist, muss der Inhaltsanbieter (hier: Hosting-Dienstleister) die URL auswerten, um die Anfrage der richtigen Internetseite zuzuordnen. Hingegen ist eine Auswertung des Inhaltes bzgl. der URL vom Zugangsanbieter zur Nachrichtenübermittlung nicht erforderlich, da das Ziel jeder Abfrage klar anhand der IP-Adresse (bzw. der Domain) zuzuordnen ist. Bei der Verwendung von Proxy-Servern u. a. beim Internetzugang per Mobilfunk ist die zuvor aufgezeigte Trennung zwischen Zugangs- und Inhaltsanbieter etwas schwieriger. Proxy-Server sind in der Lage, die Kommunikation mit dem gewählten Ziel (URL) selbst zu führen und zu beeinflussen, statt die Pakete ungesehen durchzureichen. Manche Proxy-Server ändern nicht nur das Erscheinungsbild einer Internetseite, sondern formatieren u. U. auch multimediale Inhalte (Video o. Ä.) um. Dieses Vorgehen ist vergleichbar mit der im Mobilfunk angewendeten Anpassung der Sprachcodierung während eines Telefonats. Das Auswerten der Paketinhalte kommt dem Auswerten der bei der Sprachcodierung vorgefundenen Sprachgrundfrequenz (Stimmlage) gleich, wonach es möglich wäre zu dokumentieren, ob die telefonierende Person männlich oder weiblich ist.

Die Inhalte der Datenpakete werden hier also nicht nur übermittelt, sondern auch verändert. Für die reine Datenübertragung über einen Proxy-Server wäre es ausreichend, die in den Kopfdaten der Pakete vorhandenen Ziel- bzw. Absenderadressen auszuwerten. Unabhängig davon, ob es sich um Verkehrs- oder Inhaltsdaten handelt, entbehrt die Veränderung der Daten einer Rechtgrundlage. Gleiches gilt für andere Formen der Deep Packet Inspection, mit der übermittelte oder zwischengespeicherte Inhalte ausgewertet werden können. Die Verwendung

dieser Technik durch Internetzugangsprovider und durch Anbieter von Proxy-Servern verstößt im Regelfall gegen das Fernmeldegeheimnis, sofern sie nicht ausnahmsweise für die Beseitigung einer konkreten Störung oder zur automatisierten Abwehr von Schadprogrammen erfolgt und sich auf die Auswertung von Steuerungsinformationen beschränkt.

Ich werde deshalb bei den Diensteanbietern auf die Einhaltung der rechtlichen Bestimmungen achten.

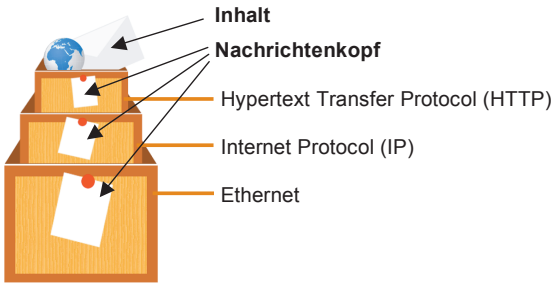
Kasten a zu Nr. 6.5

In der Netzwerktechnik steht **Deep Packet Inspection** (DPI) für ein Verfahren, mit dessen Hilfe es möglich ist, Datenpakete zu überwachen und auf verschiedenen Ebenen zu analysieren. Es können hierbei sowohl der Nachrichtenkopf als auch der Inhalt der Nachricht analysiert werden. Diese Technologie wird von Zugangs- und Inhaltsanbietern zur Vermeidung von Viren, Spam und bestimmten Protokollen, wie z. B. Voice over IP (VoIP) oder Instant Messaging, innerhalb der Datenpakete verwendet.

Für die Internetnutzung im Mobilfunk werden die Datenpakete über spezielle **Proxy-Server** geleitet, die mitunter die Inhalte der besuchten Internetseiten für die Darstellung auf (einfachen) Mobiltelefonen sowie den schnelleren Transport über das Mobilfunknetz anpassen. Der Einsatz eines Proxy-Servers für leistungsfähige Endgeräte ist der Anpassung der Daten auf die Übertragungsstrecke im Mobilfunknetz geschuldet, da hier die Verzögerungszeiten sowie die Paketverlustraten wesentlich größer sind als beispielsweise bei DSL-Anschlüssen. Bei der Verwendung von einfachen Mobiltelefonen ist es zusätzlich sinnvoll, die Darstellung der Inhalte von Internetseiten anzupassen. Entscheidungskriterium hierbei ist nicht nur die geringere Rechenleistung von Mobiltelefonen, sondern auch die geringere Displaygröße.

Kasten b zu Nr. 6.5

Verschachtelte, hierarchische Datenstruktur gängiger Kommunikationsprotokolle




Das oben stehende Bild zeigt die verschachtelte Protokollhierarchie, die notwendig ist, um z. B. eine Internetseite seite am PC zu betrachten. Jede Protokollebene bildet aus den zur Verfügung stehenden Informationen ein Datenpaket, versieht es mit Kopfdaten (vergleichbar mit Versandinformationen) und übergibt die Daten der darunterliegenden Ebene. Das Ethernet-Paket stellt in diesem Beispiel den „Transportbehälter“ für die Übertragung durch das Netzwerk dar.

## 6.6 Fluch oder Segen? Will jeder immer erreichbar sein?

*Die Eintragung von Mobilfunkanschlüssen in öffentliche Teilnehmerverzeichnisse ist die große Ausnahme. Der Gesetzgeber hat nach einem Weg gesucht, um dennoch eine größere Erreichbarkeit herzustellen. Die gesetzliche Regelung erwies sich jedoch als unpraktikabel.*

Die Anzahl der Mobilfunkanschlüsse steigt seit Jahren. Im Unterschied zu Festnetzanschlüssen sind diese Anschlüsse aber nur zu rund 5 Prozent in öffentlichen Teilnehmerverzeichnissen eingetragen, so dass die Inhaber eines Mobilfunkanschlusses in der Regel nur von Personen angerufen werden können, denen sie ihre Mobilfunknummer mitgeteilt haben. Der Gesetzgeber hat durch das Gesetz zur Änderung des Telekommunikationsgesetzes und des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmitteln vom 29. Juli 2009 (BGBl. I S. 2409 ff.) die Vorschrift des § 95 Absatz 2 TKG ergänzt, so dass es dem Diensteanbieter zukünftig möglich sein soll, einen Mobilfunkteilnehmer, der nicht in einem öffentlichen Teilnehmerverzeichnis eingetragen ist, über den individuellen Gesprächswunsch eines anderen Nutzers zu unterrichten.

Die Vorschrift des § 95 Absatz 2 TKG regelt abschließend, zu welchen Zwecken Bestandsdaten wie Telefonnummer, Name, Vorname und Anschrift eines Teilnehmers verwendet werden dürfen. Die Aufzählung zulässiger Zwecke wie Werbung, Beratung und Marktforschung wurde ergänzt um den Zweck „Unterrichtung über einen individuellen Gesprächswunsch eines anderen Nutzers“. Dies ist unkritisch, solange der Teilnehmer seine Einwilligung erteilt. Diese wiederum kann bei Neukunden problemlos bei Vertragsabschluss eingeholt werden. Anders sieht es aber bei bestehenden Kundenbeziehungen aus. Bei diesen sog. Bestandskunden darf der Diensteanbieter die Bestandsdaten nach § 95 Absatz 2 Satz 2 TKG für die Versendung einer SMS verwenden, es sei denn, der Teilnehmer hat einer solchen Verwendung widersprochen. Diese Verwendung ist nach Absatz 2 Satz 3 aber wiederum nur zulässig, wenn die entsprechende Information des Teilnehmers bei der Erhebung oder der erstmaligen Speicherung der Rufnummer oder Adresse erfolgt ist. Das Dilemma liegt auf der Hand: Zum Zeitpunkt des Vertragsabschlusses und damit der Erhebung oder erstmaligen Speicherung ihrer Daten gab es den neuen Dienst noch gar nicht. Sie konnten also zu diesem Zeitpunkt gar nicht auf eine Widerspruchsmöglichkeit hingewiesen werden. Dies hat zur Folge, dass auch bei Bestandskunden immer eine Einwilligung eingeholt werden muss und die Diensteanbieter einen hohen Kostenaufwand hätten – verbunden mit dem Risiko einer geringen Resonanz. Ob der Gesetzgeber diese Folge nicht gesehen hat oder ob er den neuen Dienst tatsächlich nur bei Vorliegen einer Einwilligung gestatten wollte, ist umstritten. Nach meiner Auffassung ist hier dem klaren Wortlaut des Geset-

zes der Vorzug zu geben. Ich würde es begrüßen, wenn die Bundesregierung eine Klarstellung im Gesetz auf den Weg bringen würde. Nur unter dieser Voraussetzung könnte ich von der Beanstandung eines entsprechenden Dienstes absehen.

## 6.7 Unterschätztes Lauschrisiko

*Das Abhören von Kommunikationsinhalten wird immer einfacher. Nicht nur drahtlose und mobile Kommunikationsmedien sind betroffen. Vorhandene Schutzmechanismen müssen eingesetzt werden – wer darauf verzichtet, handelt unverantwortlich.*

Durch einen betrieblichen Datenschutzbeauftragten wurde ich auf einen Abhörfall in der Kabelkommunikation aufmerksam gemacht. Ein lokales Telekommunikationsunternehmen offerierte ein Telefon- und Internet-Angebot über das eigene Kabelnetz. Hierzu wurden zunächst Testkundenvereinbarungen abgeschlossen. Problematisch war, dass die Telefonate der Testkunden nicht verschlüsselt waren und zumindest über ein Vierteljahr abgehört werden konnten. Das Abhören war, so die nachvollziehbare Aussage bei den Ermittlungen der Staatsanwaltschaft, mittels einfacher Hardware (z. B. PC mit DVB-C-Karte) und im Internet verfügbarer Software möglich. Die unverschlüsselten Telefonate konnten zunächst im gesamten Netz, später noch in größeren Segmenten empfangen werden.

Gemäß § 109 Absatz 1 TKG hat jeder Diensteanbieter angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze des Fernmeldegeheimnisses und personenbezogener Daten und der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen. Im konkreten Testbetrieb wurden die Teilnehmer entgegen der Informationsverpflichtung aus § 93 Absatz 2 TKG nicht in allgemein verständlicher Form über die besonderen Risiken der Netzsicherheit aufgeklärt. Das Telekommunikationsunternehmen hat sein Telefon- und Internet-Angebot zwischenzeitlich nachgebessert und den verschlüsselten Regelbetrieb aufgenommen.

Ein Petent berichtete mir davon, dass sein DSL-Anschluss (vgl. Kasten zu Nr. 6.7) von „fremden“ Daten ausgebremst wird. Nach seiner Auskunft gestaltete sich die Störung so, dass der Downstream (Kanal, in dem die Daten vom DSL-Anbieter zum Kunden fließen) bereits im Ruhezustand eine beträchtliche Menge an ankommenden Daten aufwies, die ihn hinderte, im Internet zu surfen bzw. zu telefonieren. Seine Analyse der ankommenden Daten ergab, dass es sich um Daten handelte, die für einen bzw. mehrere andere Kunden des DSL-Anbieters gedacht und entsprechend adressiert waren. Während der Analyse war der Petent nach eigenen Angaben in der Lage, den Inhalt der Datenpakete zu entziffern und z. B. Telefongespräche (VoIP) mitzuhören. Eine intensive Untersuchung förderte zu Tage, dass sowohl eine unzureichende (bzw. sehr offene) Konfiguration der Hardware in der Vergangenheit zu (unbeabsichtigtem) unberechtigtem Zugriff führte, als auch Hardwaredefekte diese und ähnliche Symptome aufweisen.

Bereits 2009 wurde bekannt, dass über DECT (Digital Enhanced Cordless Telecommunications) geführte Telefonate mit geringem Kostenaufwand und wenig Vorkenntnissen abgehört werden können. Dies liegt darin begründet, dass zum einen die Kosten für die zum Abhören erforderliche Hardware gefallen sind und zum anderen die meisten Hersteller aktueller DECT-Produkte wider besseren Wissens die optional für DECT standardisierte Verschlüsselung nicht einsetzen. Für die Nutzer ist es dabei nicht einmal erkennbar, ob ein von ihnen verwendetes Gerät die Verschlüsselungsmöglichkeiten von DECT nutzt oder ob die Daten völlig unverschlüsselt übertragen werden.

Im Mobilfunk ist die Situation ebenfalls unbefriedigend. Zwar wird beim Mobilfunk (hier: GSM) flächendeckend die Verschlüsselung eingesetzt, aber der verwendete Algorithmus genügt aufgrund seines „Alters“ nicht mehr den aktuellen Ansprüchen an die Abhörsicherheit. Im Dezember 2009 zeigten Computerexperten eine kostengünstige Möglichkeit, Mobiltelefonate in weniger als 20 Minuten zu entschlüsseln.

Insgesamt beobachte ich die derzeitige Situation hinsichtlich der Abhörsicherheit von Kommunikationsinhalten mit Sorge, zumal die rasante Entwicklung technischer Möglichkeiten zur Kommunikationsüberwachung noch Schlimmeres befürchten lässt. Der durch die breite Verfügbarkeit von technischen Einrichtungen zum Abhören und Entschlüsseln drahtloser Kommunikation steigenden Unsicherheit könnte sehr einfach durch den Einsatz bzw. das Einbringen aktueller Verschlüsselungsalgorithmen begegnet werden. Ich halte es für unverantwortlich, dass die meisten Hersteller von schnurlosen Telefonen aus rein wirtschaftlichen Gründen ihre Geräte ohne die im DECT-Standard enthaltene Verschlüsselung auf den Markt bringen und dies nicht einmal kenntlich machen. Zudem ist daran zu erinnern, dass gemäß § 109 Absatz 1 TKG alle Diensteanbieter für den Schutz der Inhaltsdaten zu sorgen haben, indem sowohl die korrekte Konfiguration als auch die Funktionsfähigkeit der Hardware sichergestellt ist.

Kasten zu Nr. 6.7

Ein DSL-Anschluss ist derart gestaltet, dass die Teilnehmeranschlussleitungen (TAL) mehrerer Kunden eines Anbieters in der Vermittlungsstelle ankommen, wo das DSL-Signal zunächst vom Telefonsignal getrennt wird. Die gesammelten DSL-Anschlüsse werden dem Digital Subscriber Line Access Multiplexer (DSLAM) zur Verfügung gestellt, welcher für den Anschluss vieler Kunden an das Netz des Anbieters sorgt. Die darauf folgende Netzkomponente ist der DSL-Access Concentrator (DSL-AC), welcher den Übergang in das Internet bereitstellt.

In der „klassischen“ DSL-Infrastruktur werden die Kundendaten vom DSL-Modem mehrfach verpackt und per Asynchronous Transfer Mode (ATM) bis zum DSL-ACn einer Punkt-zu-Punkt-Verbindung übertragen. Das ATM-Funktionsprinzip sichert hier durch einen privaten (virtuellen) Kanal die Daten vor den „Blicken“ anderer Kunden.

In den sog. Next Generation Networks (NGN), welche häufig von Anbietern eingesetzt werden, die über keine ei-

eigenen Leitungen verfügen, werden die Netzwerke, unabhängig von deren Infrastruktur, zum Teil mit dem Ethernet-Protokoll betrieben. Im Gegensatz zu den klassischen Netzen wird hier die ATM-Struktur bereits im DSLAM aufgelöst und die Daten als Ethernetpakete weiter zum DSL-AC übertragen. Diese Kommunikation ist prinzipiell verbindungslos, d. h. die Pakete vieler Kunden werden auf einer gemeinsamen Verbindung übertragen, was die Trennung zwischen den Kunden technisch schwierig gestaltet.

## 6.8 Der E-Postbrief ist unterwegs – kommt er auch sicher an?

*Die Deutsche Post AG hat meine Empfehlungen zur Konzeption und den Datenschutzhinweisen weitgehend berücksichtigt.*

Seit dem Sommer 2010 bietet die Deutsche Post AG eine neue Versendungsform an, den E-Postbrief. Das Unternehmen hatte mir die neue Dienstleistung vor der Praxiseinführung vorgestellt. Der E-Postbrief bietet zusätzlich zum herkömmlichen papierbasierten Brief die Möglichkeit zur Übermittlung von Briefen in elektronischer Form. Zur Teilnahme am Verfahren, ob als Absender oder Empfänger, ist eine individuelle Registrierung erforderlich. Es gibt zwei Versandwege: Zum einem den vollelektronischen Versandweg, bei dem der vom Absender verfasste elektronische Brief unmittelbar an den Empfänger versendet wird. Bei dem anderen Versandweg ist nur der Absender, nicht aber der Empfänger registrierter Teilnehmer des E-Postbrief-Verfahrens. Bei diesem sog. Hybridbrief wird der vom Absender elektronisch erstellte Brief durch die Deutsche Post AG ausgedruckt, kuvertiert und dem Empfänger auf dem normalen Postweg zugestellt (vgl. Kasten zu Nr. 6.8).

Bei der vollelektronischen Übermittlung des E-Postbriefs (Absender und Empfänger sind registriert) ist die Vertraulichkeit derzeit technisch nicht vollständig gewahrt, da auf eine Ende-zu-Ende-Verschlüsselung verzichtet wird. Der Absender muss daher – wie bei der De-Mail (vgl. unter Nr. 3.3) – bei Daten mit erhöhtem Schutzbedarf (z. B. sensible Gesundheitsdaten) zusätzliche, eigene Maßnahmen, wie z. B. das Anfügen dieser Daten in einem verschlüsselten Anhang ergreifen. Beim Hybridbrief soll die vertrauliche Behandlung der übermittelten Daten gewährleistet werden, indem die mit dem Ausdruck der Briefe betrauten Mitarbeiter/innen sich strafbar machen, falls sie das Post- und Fernmeldegeheimnis (Art. 10 GG) verletzen würden.

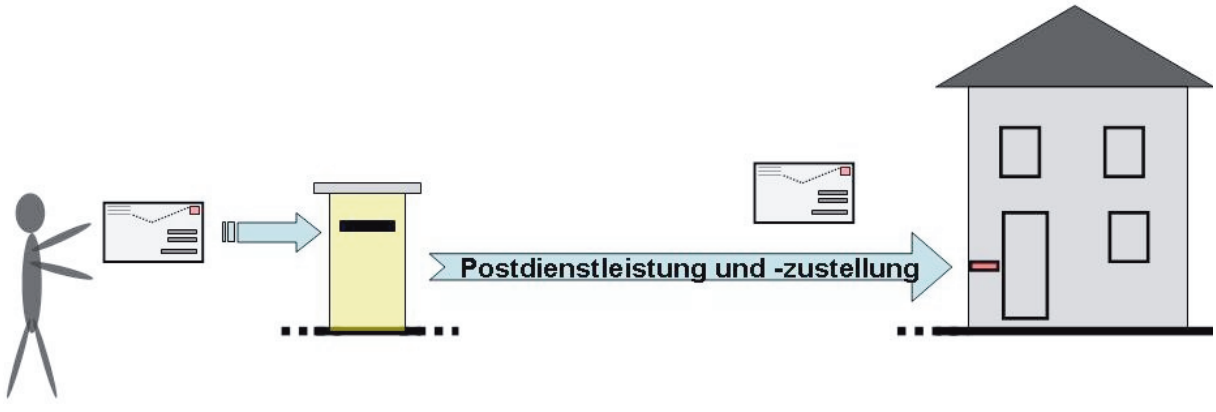
Ende Oktober 2010 habe ich sowohl das Rechenzentrum, das die Applikationen und die digitale Abwicklung bereitstellt, als auch ein Druckzentrum besichtigt, in dem der Hybridbrief versandt werden soll. Bei beiden Informationsbesuchen traten keine datenschutzrechtlichen Probleme zutage. In dem Druckzentrum werden bereits seit langem andere Dokumente mit teils sensiblen Inhalten wie Rechnungen oder Kontoauszüge im Auftrag zahlreicher Unternehmen ausgedruckt.

Bislang liegen mir nur wenige Eingaben zum E-Postbrief vor. Diese befassen sich überwiegend mit dem Registrierungsverfahren (Pflichtangabe einer Handynummer für das TAN-Verfahren) und dem Ausdruck des E-Postbriefs durch die Deutsche Post AG, wenn eine Zustellung nur auf dem „normalen Postweg“, also als Hybridbrief, möglich ist. Hier bestanden u. a. Bedenken, ob das Postgeheimnis gewahrt wird. Der Beförderungsvertrag wird nur zwischen dem Absender und der Deutschen Post AG abgeschlossen, so dass der Empfänger auf die Versandform keinen Einfluss hat. Da der Ausdruck des Briefes im Rahmen eines Auftragsverhältnisses durch die Deutsche Post AG erfolgt, bleibt diese aus datenschutzrechtlicher Sicht die verantwortliche Stelle für die Einhaltung des Postgeheimnisses.

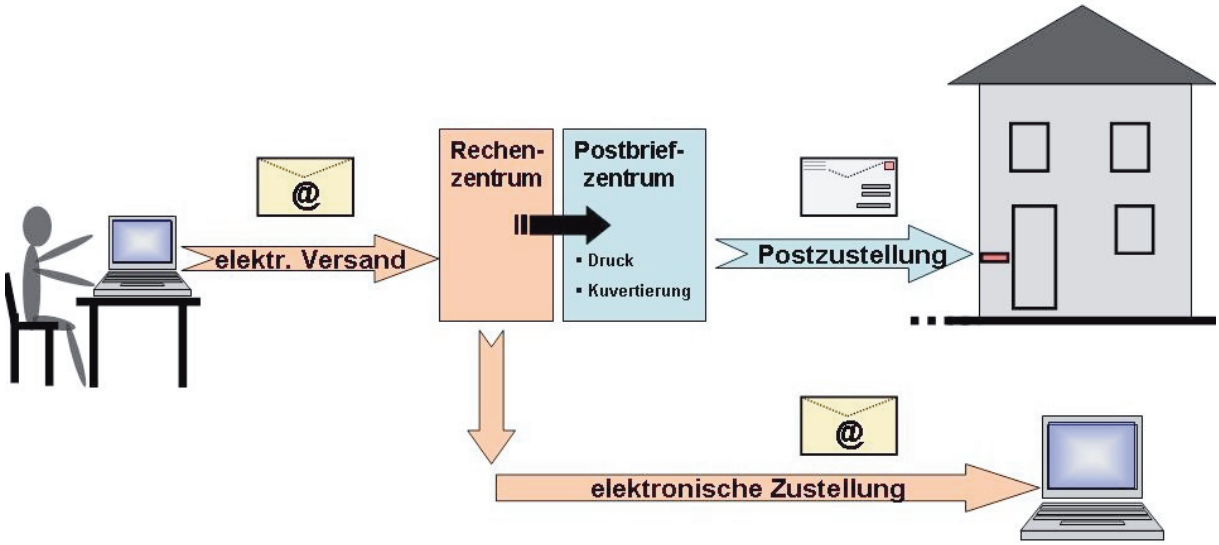
Kasten zu Nr. 6.8

Der E-Postbrief im Vergleich zur konventionellen Postzustellung:

Versandweg beim konventionellen Brief:



Versand beim E-Postbrief:




Im Gegensatz zum konventionellen Brief wird der E-Postbrief elektronisch erstellt und verschickt. Die Zustellung erfolgt bei einem registrierten Empfänger in elektronischer Form. Bei Zustellung an nicht registrierte Teilnehmer wird die Sendung in einem Postbriefzentrum ausgedruckt, kuvertiert und auf dem herkömmlichen Weg zugestellt (sog. Hybridbrief).

## 6.9 Sorgfaltspflichten der Telekommunikationsunternehmen gegenüber ihren Kunden

*In einem Urteil des Landgerichts Bonn vom 1. Juni 2010 (7 O 470/09) wurde einem Telekommunikationsunternehmen die Pflicht auferlegt, seine Kunden schnellstmöglich auf ungewöhnlich hohe Rechnungsbeträge hinzuweisen. Ungeklärt blieb aber die Frage, ob und wie dies datenschutzkonform zu bewerkstelligen ist.*

Eine Kundin verklagte ihren Telekommunikationsanbieter auf Rückzahlung von zu hohen Rechnungsbeträgen. Unstrittig war, dass die in Rechnung gestellten Kosten tatsächlich angefallen waren, weil die Kundin einen Internettarif nutzte, der minutenweise abgerechnet wurde. Der ihr vom Telekommunikationsanbieter überlassene Router war aber so konfiguriert, dass er – auch wenn tatsächlich keine Nutzung des Internets erfolgte – ständig eine Verbindung aufrecht erhielt. Hierdurch summierten sich die Kosten innerhalb von fünf Monaten auf über 5 000 Euro. Das Gericht gab der Klage der Kundin statt. Dem Telekommunikationsanbieter erwachse aus dem vertraglichen Dauerschuldverhältnis mit der Kundin eine besondere Fürsorgepflicht, die ihn dazu verpflichtet, auf ungewöhnliches Nutzungsverhalten der Kundin innerhalb weniger Tage zu reagieren.

Das Gericht setzte sich allerdings nicht damit auseinander, wie die faktische Umsetzung dieser schuldrechtlichen Verpflichtung gesetzeskonform erfolgen soll. Das Telekommunikationsgesetz (TKG) setzt Telekommunikationsanbietern klare Grenzen, innerhalb derer sie die Bestands- und Verkehrsdaten ihrer Kunden verwenden dürfen. Eine hier naheliegende dauerhafte Überwachung der Verkehrsdaten ist in diesem Fall nicht zulässig. Die Vorschrift des § 100 Absatz 3 TKG, nach der eine Verkehrsdatenverarbeitung zur Erkennung von Missbrauch in Telekommunikationsnetzen zulässig ist, kann hier nicht zur Anwendung kommen, da kein Missbrauchsfall, sondern lediglich ein fehlerhaft eingestellter Router Grund für die hohe Rechnung war.

Eine Nutzungskontrolle könnte aus meiner Sicht allenfalls über die Rechnungsdaten selbst erfolgen, die im Rahmen des Vertragsverhältnis erhoben werden und somit als für die Erbringung des Telekommunikationsdienstes erforderliche Bestandsdaten im Sinne des § 95 Absatz 1 TKG verwendet werden dürfen. Sollte ein Telekommunikationsanbieter im Rahmen einer solchen Rechnungskontrolle ein atypisches Nutzungsverhalten eines Kunden feststellen, darf er diesen hierüber informieren. Weitere über diese Information hinausgehende Maßnahmen, insbesondere die Einsicht in Verkehrsdaten, um festzustellen, worin die konkrete Ursache für die Auffälligkeit liegt, sind jedoch ausschließlich unter der Voraussetzung einer hierzu vom Kunden erteilten expliziten Einwilligung möglich. Für Telekommunikationsanbieter bleibt die missliche Lage, unter dem Damoklesschwert solcher Urteile leben zu müssen, die kaum datenschutzkonform umzusetzen sind.

## 6.10 Neuvergabe von E-Mail-Adressen

*Bei einer zu schnellen Neuvergabe von E-Mail-Adressen können Nachrichten an den falschen Empfänger gelangen. Ich halte eine Karenzzeit von mindestens drei Monaten für angebracht.*

Viele Bürger beklagten in Eingaben an meine Dienststelle, dass die von ihnen nach Vertragsbeendigung aufgegebene E-Mail-Adresse sehr kurzfristig an einen neuen Kunden vergeben wurde und somit Nachrichten an den falschen Empfänger gelangten. Dem Absender war dies in der Regel nicht bekannt, denn anders als etwa bei der Telefonie fehlt es hier an einem direkten Kontakt mit dem Empfänger.

Grundsätzlich ist jeder Nutzer selbst gehalten, seine Kontaktpersonen darüber zu informieren, dass eine bestimmte E-Mail-Adresse nicht mehr gültig ist. Gleichwohl habe ich Verständnis dafür, dass dies nicht in jedem Einzelfall möglich ist. Ich halte deshalb die auf dem 47. Meeting der International Working Group on Data Protection in Telecommunications erarbeitete Empfehlung, E-Mail-Adressen erst nach einer Wartezeit von drei Monaten wieder zu vergeben, für angemessen. Den deutschen Anbietern von E-Mail-Adressen habe ich empfohlen, ihre Praxis an dieser Empfehlung auszurichten.

### 6.11 Elektronische Sortierung und Stichprobenerhebung von Postsendungen

*Bei der Einführung neuer Verfahren und Techniken wenden sich Postdienstleister vielfach an mich, um sie bei der Einhaltung datenschutzrechtlicher Bestimmungen zu unterstützen, so auch die Deutsche Post AG vor der Einführung einer Mail Sampling Unit.*

Im vergangenen Jahr informierte mich die Deutsche Post AG über ihre Absicht, Postsendungen im internationalen Postverkehr mittels entsprechender Technologie in einer neuartigen Sortieranlage (Mail Sampling Unit – MSU) stichprobenartig zu fotografieren und diese Fotos für eine Dauer von zwei Jahren bis zum Jahresende zu speichern, um die Abrechnung mit ausländischen Postgesellschaften bezüglich fehlgeleiteter Sendungen zu verbessern.

Zurzeit erfolgt diese Abrechnung gemäß internationaler Vereinbarungen (z. B. Weltpostvertrag) durch eine Schätzung der jährlichen Anzahl solcher fehlgeleiteten Postsendungen. Aufgrund des zunehmenden Marktdrucks hat die Reklamation solcher Abrechnungen auch gegenüber der Deutsche Post AG erheblich zugenommen. Ein anderes internationales Postunternehmen habe mit dieser Methode bereits die Richtigkeit seiner Zählergebnisse nachgewiesen und damit seine Verhandlungsposition im Abrechnungsverfahren verbessert.

Mit dem Einsatz der MSU solle daher auch bei der Deutsche Post AG das bisherige Schätzverfahren durch eine exakte und beweissichere Erfassung fehlgeleiteter Postsendungen ersetzt werden. Die Deutsche Post AG sieht vor diesem Hintergrund das MSU-Verfahren als erforderlich im Sinne von § 5 Absatz 4 Postdienste-Datenschutzverordnung an. Hiernach dürfen Diensteanbieter personenbezogene Daten erheben, verarbeiten und nutzen, soweit es zum ordnungsgemäßen Ermitteln, Abrechnen und Auswerten sowie zum Nachweis der Richtigkeit von Leistungsentgelten erforderlich ist. Dabei ist an die Erforderlichkeit ein strenger Maßstab anzulegen. Bei der Beurteilung ist zu berücksichtigen, dass die (digitale) Dokumentation zu einer umfassenden Registrierung bei aus dem Ausland eingehenden Postsendungen führen würde. Dies hätte erhebliche Auswirkungen auf das informationelle Selbstbestimmungsrecht sowohl der Absender als auch der Empfänger von Postsendungen.

Da das bisherige Schätzverfahren bei der Abrechnung im internationalen Postverkehr noch nicht verbindlich durch das elektronische Abrechnungsverfahren abgelöst wurde, halte ich es bis auf weiteres nicht für erforderlich, einer ausländischen Postgesellschaft im Streitfall jedenfalls solche beweissichernden Sendungsfotos vorzulegen, die auch den Namen und die Anschrift des Sendungsempfängers enthalten.

Ich habe die Deutsche Post AG deshalb aufgefordert zu prüfen, ob – sofern am Einsatz der MSU festgehalten wird – die Erfassung der Sendungsbilder so gestaltet werden kann, dass nur die zu Abrechungszwecken tatsächlich erforderlichen Daten wie Bestimmungsland, -ort und Postleitzahl in die Erhebung einfließen. Eine Antwort der Deutsche Post AG steht noch aus, sodass mir eine abschließende Bewertung noch nicht möglich ist.

### 6.12 Sendungsverfolgung und ZORA: „Datenschlankheitskur“ bei der Deutsche Post AG

*Die Sendungsverfolgung der Deutsche Post AG wurde nach mehreren Pannen datenschutzgerecht umstrukturiert. Der Umfang der hierfür und bei der Abholung nachweispflichtiger Sendungen gespeicherten Daten wurde reduziert.*

Viele Menschen freuen sich über die Möglichkeit, nachvollziehen zu können, wo die von ihnen aufgegebenen oder an sie gerichteten Postsendungen sich gerade befinden. Andere stören sich daran, dass bisweilen nicht nur sie diese Informationen erhalten, sondern auch unberechtigte Dritte.

Seit der Einführung der Sendungsverfolgung der Deutsche Post AG erreichten mich immer wieder Beschwerden, in denen die Möglichkeit zur Einsichtnahme in Sendungsdaten Dritter beklagt wurde (vgl. 20. TB Nr. 14.2). Die Sicherheitsmängel hatten verschiedene Ursachen:

- Der Identcode der Sendung wurde vom Geschäftskunden zu früh an den Endkunden weitergegeben, so dass der Empfänger noch nicht die Daten der an ihn gerichteten Sendung, eventuell aber Altdaten über früher unter diesem Identcode abgewickelten Sendungen Dritter finden konnte. Zum Teil waren diese Daten älter als zwölf Monate.
- Geschäftskunden verwendeten mehrmals hintereinander denselben Identcode.
- Die Anforderungen an das Passwort für Geschäftskunden entsprachen nicht den Datensicherheitsanforderungen.

Nach Bekanntwerden dieser Probleme hat die Deutsche Post AG Maßnahmen ergriffen, um die so verursachte datenschutzwidrige Einsichtnahme in dem Postgeheimnis

(§ 39 Absatz 1 und 2 Postgesetz) unterliegende Sendungsdaten abzustellen:

- Die Vergabe des Passworts für Geschäftskunden wurde an datenschutzrechtliche Vorgaben angepasst.
- Die Anzahl der Ziffern der Sendungsnummern wurde erhöht, um den Geschäftskunden mehr Sendungsnummern zur Verfügung stellen zu können. Dadurch wurden die Fälle einer Mehrfachvergabe der Sendungsnummern für die Dauer der Anzeige im System reduziert.
- Der Zeitraum der Anzeige wurde auf drei Monate begrenzt.
- Die Sendungsverfolgung mit einem Mehrfachaufruf (alle Sendungen des Versenders werden angezeigt) wurde so konfiguriert, dass bei Vorliegen älterer und neuerer Informationen zu einer Sendungsnummer nur die neueren angezeigt werden. Bei Fragen zu älteren Sendungsdaten muss der Kundenservice der Deutsche Post AG kontaktiert werden.

Schließlich wurde die Anzeige der Daten bei der Sendungsverfolgung auf Sendungsnummer, Sendungsverlauf und Zustellstatus beschränkt.

Zudem hat die Deutsche Post AG die Ausweisdatenerhebung bei der Paketabholung reduziert. Wenn der Empfänger die Sendung selbst abholt, wird nur noch Einsicht in sein Ausweisdokument genommen und dies vermerkt. Eine Speicherung von Ausweisdaten findet nicht mehr statt. Bei Abholung durch einen Bevollmächtigten des Empfängers werden die Ausweisdaten auch weiterhin zulässigerweise erhoben und gespeichert.

Ich begrüße die genannten Maßnahmen, da sie die Einsichtnahme in die Daten Dritter verhindern und den Umfang der gespeicherten Daten verringern.

### *Freiheit und Sicherheit*

## 7 Innere Sicherheit

### 7.1 Sicherheitsarchitektur des Bundes

#### 7.1.1 Evaluierung von Sicherheitsgesetzen – Sichere Entscheidungsgrundlagen für Grundrechtsschutz und Effizienz

*Die Evaluierung von Sicherheitsgesetzen soll dem Gesetzgeber eine solide Wissensgrundlage für weitere Entscheidungen geben. Dabei sind hohe Anforderungen an Methodik und Maßstäbe zu richten.*

In der Vergangenheit wurden den Sicherheitsbehörden auf Grund aktueller Gefährdungslagen und zugespitzter Risikowahrnehmung wiederholt zusätzliche Befugnisse eingeräumt. Die entsprechenden gesetzlichen Grundlagen wurden dabei bisweilen in großer Eile formuliert und beraten. Es nimmt nicht Wunder, dass dabei immer wieder handwerkliche Fehler passieren. Noch bedenklicher ist, dass im Eilverfahren in Grundrechte eingegriffen wurde. Immer wieder hat das Bundesverfassungsgericht deshalb den Gesetzgeber korrigiert, etwa beim Großen Lauschangriff (vgl. 20. TB Nr. 7.1.1), bei der Telefonüberwachung durch das Zollkriminalamt (vgl. 20. TB Nr. 5.4.3), bei der Online-Durchsuchung (vgl. 22. TB Nr. 4.1.1) und zuletzt bei der Vorratsdatenspeicherung (vgl. Nr. 6.1).

Deshalb ist es dringend geboten, die neuen Befugnisse im Lichte der seit ihrer Einführung gewonnenen Erfahrungen einer kritischen Überprüfung zu unterziehen. Fachleute sprechen hier von „Evaluierung“.

Verschiedene gesetzliche Regelungen zu Befugnissen im Bereich der Sicherheitsbehörden verpflichten Bundesregierung und Gesetzgeber zur Evaluierung. Dies betrifft das Terrorismusbekämpfungsergänzungsgesetz (vgl. 21. TB Nr. 5.1.2) zum 9. Dezember 2010, das Antiterrordateigesetz (vgl. 21. TB Nr. 5.1.1) zum 31. Dezember 2011 und das BKA-Gesetz (vgl. 22. TB Nr. 4.3.1) hinsichtlich der dem Bundeskriminalamt übertragenen Aufgabe der Abwehr von Gefahren des internationalen Terrorismus und den ihm hierfür eingeräumten Befugnissen zur Rasterfahndung und zur sog. Online-Durchsuchung zum 1. Januar 2014. Darüber hinaus sind im Koalitionsvertrag der derzeitigen Bundesregierung weitere Evaluierungen vereinbart worden. So will die christlich-liberale Regierungskoalition Aufgaben und Zuständigkeiten der Sicherheitsbehörden, die Reform der Telekommunikationsüberwachung sowie die Sicherheitsdateien unter dem Blickwinkel des Trennungsgebotes zwischen Polizei und Nachrichtendiensten evaluieren.

Dem Gesetzgeber obliegt – besonders im grundrechtsrelevanten Bereich – nach der ständigen Rechtsprechung des Bundesverfassungsgerichts die Pflicht, die Auswirkungen seiner Gesetze in der Praxis fortlaufend zu beobachten und die Vorschriften gegebenenfalls nachzubessern. Dies gilt insbesondere dann, wenn neue Befugnisse eingeführt werden, deren Auswirkungen zum Zeitpunkt des Gesetzgebungsverfahrens noch nicht absehbar sind. Die Einschätzungsprärogative des Gesetzgebers korrespondiert also mit nachträglichen Kontrollpflichten.

Diese verfassungsrechtliche Notwendigkeit ist auch politisch von großer Bedeutung. Eine Evaluierung hat den Zweck, dem Gesetzgeber eine tatsächliche und wissenschaftlich fundierte Grundlage für künftige Entscheidungen zu geben. Nur auf diese Weise kann er Gesetze schaffen, die einerseits Eingriffe in die Grundrechte – insbesondere unbeteiligter Bürgerinnen und Bürger – so gering wie möglich halten und andererseits den Sicherheitsbehörden gleichzeitig ermöglichen, ihre Aufgaben effektiv wahrnehmen zu können. Evaluierung verbindet Grundrechtsschutz mit einer Effizienzsteigerung der sicherheitsbehördlichen Arbeit. Sie kann z. B. dazu führen, dass Ressourcen zielgerichteter eingesetzt werden, z. B. für Terrorismusbekämpfung. Evaluierung kann aber auch ergeben, dass Eingriffsbefugnisse enger ausgestaltet oder Datenbestände verkleinert werden. Die Diskussion darüber könnte heute womöglich mit größerer Standfestigkeit geführt werden, wenn man bereits früher in größerem Umfang Evaluierungen durchgeführt hätte.

Evaluierungsvorhaben werden aber ihr Ziel nicht erreichen, wenn ihre Methodik und die angelegten Maßstäbe zu eng ausgestaltet sind.

Aufgrund der Eingriffsintensität der Regelungen und Verfahren im Bereich der Sicherheitsbehörden halte ich eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes für unabdingbar. Eine Evaluierung ist erst dann aussagekräftig, wenn diese durch eine unabhängige Stelle nach wissenschaftlichen Methoden durchgeführt wird. Sie darf nicht interessengeleitet erfolgen, weshalb eine rein (regierungs-)interne Evaluation ausscheidet. Eine interne Durchführung würde auch den gesetzlichen Anforderungen nicht genügen, da die bisherigen Regelungen die „Einbeziehung" eines wissenschaftlichen Sachverständigen einfordern. Ebenfalls nicht ausreichend wäre es, wenn die Ressorts nur eine externe „Methodenberatung" einholen oder den Evaluierungsmaßstab selbst festgelegen würden.

Die Auswirkungen auf die Betroffenen bzw. auf die Grundrechte sollte Kernbestandteil jeder Evaluierung sein. Dies erfordert eine umfassende rechtliche und verfassungsrechtliche Überprüfung auf Basis einer vollumfänglichen rechtstatsächlichen Analyse. Die Verhältnismäßigkeit der zu evaluierenden Sicherheitsgesetze ist dabei vollständig auf den Prüfstand zu stellen. Dabei muss gründlich untersucht werden, ob die tatsächlich erreichten Auswirkungen über das definierte Ziel hinausgehen und welche Wirkungen sie für die Betroffenen in der Lebenswirklichkeit hatten. Im Sinne einer Gesamtbetrachtung ist in den Blick zu nehmen, wie tief und mit welcher Streubreite die zu evaluierenden Befugnisse – auch im Zusammenwirken mit anderen Befugnissen – in die Privatsphäre der Menschen eindringen.

Völlig unzureichend wäre es hingegen, den Schwerpunkt einer Evaluierung nur auf den Bereich der Zweckerreichung im praktischen Vollzug zu legen, ohne dass rechtliche Wertungen auch hinsichtlich der Auswirkungen auf die Betroffenen nachvollzogen werden. Auch eine Beschränkung auf formale Gesichtspunkte des Trennungsgebotes würde dessen grundrechtliche Bedeutung außerachtlassen, die das Bundesverfassungsgericht ausdrücklich hervorgehoben hat.

Ich halte es für geboten, diese Aspekte im Rahmen der anstehenden Evaluierungen zu berücksichtigen und habe die Bundesregierung hierauf auch mehrfach hingewiesen. Auch die 79. Konferenz der Datenschutzbeauftragten hat in einer Entschließung eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich gefordert (vgl. Kasten zu Nr. 7.1.1).

Weil einerseits die Evaluierung von Gesetzen zunehmend an Bedeutung gewinnt, andererseits aber z. T. erhebliche Unsicherheiten bzw. Meinungsdivergenzen zu Inhalten und Verfahren bestehen, habe ich dem Deutschen Forschungsinstitut für Öffentliche Verwaltung Speyer einen Forschungsauftrag zu der Thematik erteilt. Ich hoffe, dass damit die Gesetzesevaluierung auf eine bessere, d. h. wissenschaftliche Grundlage gestellt werden kann, dem Gesetzgeber im Hinblick auf zukünftige Evaluierungsvorhaben verfassungsrechtlich gebotene Inhalte bzw. Konkretisierungen vermittelt werden und dies zu einer Vereinheitlichung der Evaluierung von Gesetzen beiträgt (vgl. auch Nr. 14.6).

Kasten zu Nr. 7.1.1

**Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010**

**Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich**

Die Bundesregierung beabsichtigt, nicht nur die in den vergangenen Jahren durch zahlreiche Gesetze neu geschaffenen Befugnisse und die bestehenden Sicherheitsdateien, sondern auch die Kooperationszentren, in denen Polizei und Nachrichtendienste zusammenarbeiten, zu evaluieren.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, die Evaluierung zeitnah und vorbehaltlos nach wissenschaftlichen Kriterien durchzuführen. Kein Vorbild darf die im Mai 2005 vorgenommene „Evaluierung" des Terrorismusbekämpfungsgesetzes 2002 sein. Diese war eine inhaltlich und methodisch defizitäre Selbsteinschätzung. Dagegen enthalten die in verschiedenen Gesetzen aufgenommenen Evaluationsklauseln sinnvolle Ansätze, die es weiter zu entwickeln gilt. Dies betrifft etwa die Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt darauf hingewiesen, dass die Ausweitung der Befugnisse von Polizei und Verfassungsschutz, auch in das Vorfeld der Gefahrenabwehr, zur anlasslosen, oftmals massenhaften Erhebung personenbezogener Daten unbescholtener Bürgerinnen und Bürger führen kann.

Aufgrund der Eingriffsintensität der Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

### 7.1.2 Kontrolle der Anti-Terror-Datei bei den Nachrichtendiensten des Bundes

*Die Datenverarbeitung durch BfV in der Anti-Terror-Datei weist erhebliche Mängel auf.*

Nachdem ich die Datenverarbeitung durch das BKA in der Anti-Terror-Datei überprüft hatte (vgl. 22. TB Nr. 4.2.2.2), bildete diesmal die Kontrolle der entsprechenden Datenverarbeitung durch BfV und BND einen Schwerpunkt meiner Tätigkeit. Dabei habe ich zum Teil erhebliche Mängel festgestellt:

Auch beim BfV wird die ATD über eine von ihr geführte Quelldatei automatisiert befüllt. Dies führt zu Problemen bei der Übertragung erweiterter Grunddaten. So dürfen bestimmte Daten, die zulässigerweise in der Quelldatei gespeichert sind, wegen der restriktiveren Regelungen des Anti-Terror-Datei-Gesetzes (ATDG) nicht in die ATD aufgenommen werden. Hier bedarf es einer differenzierteren Selektion vor der Übertragung der Daten in die ATD. Zudem habe ich festgestellt, dass Datensätze, die in der Quelldatei zur Löschung anstanden, weiterhin in der ATD vorgehalten wurden, und Freitextfelder unzulässige Bearbeitervermerke enthielten.

Erfreulicherweise ist das BfV problembewusst und hat zugesagt, die Defizite nicht nur systemseitig zu beheben, sondern auch durch besondere Schulungsmaßnahmen künftig die ordnungsgemäße Befüllung der ATD sicherzustellen.

Entgegen den im ATDG normierten gesetzlichen Voraussetzungen hat das BfV sämtliche Daten, die durch heimliche Telekommunikationsüberwachungen erhoben worden sind und daher besonders gekennzeichnet werden müssen, ungekennzeichnet in der ATD gespeichert. Folge: Die anderen ATD-Behörden haben diese Daten ungekennzeichnet weiter verwendet. Ohne die Kennzeichnung ist für Niemanden mehr erkennbar, dass es sich um gesetzlich besonders geschützte Daten handelt, die nur unter besonderen Voraussetzungen verarbeitet werden dürfen. Das System des BfV, das die Daten aus den Quelldateien in die ATD überträgt, sah keine derartige Kennzeichnung vor. Hiervon war eine Vielzahl von Daten betroffen. Auf meine Aufforderung hin hat das BfV zugesagt, unverzüglich die gesetzlich vorgeschriebene Kennzeichnung durchzuführen und zu gewährleisten, dass sämtliche Empfänger über ihre Kennzeichnungspflicht unterrichtet werden. Auf eine formelle Beanstandung habe ich deshalb verzichtet. Ich werde die Umsetzung der Zusagen kontrollieren.

Als ein weiterhin ungelöstes datenschutzrechtliches Problem erweist sich die Bewertung, wann eine Kontaktperson als „dolos“ im Sinne des ATDG einzustufen ist. „Dolos“ bedeutet, dass bei den betreffenden Personen tatsächliche Anhaltspunkte dafür vorliegen müssen, dass sie von der Planung oder Begehung einer terroristischen Straftat oder der Ausübung, Unterstützung oder Vorbereitung von rechtswidriger Gewalt im Sinne des ATDG Kenntnis haben. Dadurch kann sich der Umfang der erfassten Daten erheblich vergrößern und entsprechend tiefer in das informationelle Selbstbestimmungsrecht der betreffenden Person eingegriffen werden. Entgegen der Auffassung des BfV reicht dabei nachrichtendienstliches Erfahrungswissen für die Schwelle der Dolosität nicht aus. Vielmehr ist angesichts der Grundrechtsintensität einer ATD-Speicherung die Verbindung zu einer konkreten Handlung, die wissentlich unterstützt wird, zwingend erforderlich.

Die Auswertung des im Rahmen der Kontrolle der Datenverarbeitung des BND in der ATD erlangten Materials war bei Redaktionsschluss noch nicht abgeschlossen. Das Ergebnis werde ich im nächsten Tätigkeitsbericht erörtern.

### 7.1.3 Protokollierung bei den Sicherheitsbehörden

Die zunehmende informationelle Vernetzung der Sicherheitsbehörden sowie die Errichtung von Großdateien bei den Polizeien und Nachrichtendiensten des Bundes machen es erforderlich, neue Wege für eine sachgerechte Datenschutzkontrolle bei den jeweiligen Behörden zu beschreiten. Eine Möglichkeit liegt in der stärkeren Nutzung der bei dem Betrieb von Datenbanksystemen anfallenden Protokolldaten. Voraussetzung hierfür ist aber eine vollständige inhaltliche Protokollierung aller Datenbanktransaktionen zu Zwecken des Datenschutzes (vgl. o. Nr. 5.7).

### 7.1.4 Das Gemeinsame Internetzentrum (GIZ) der Sicherheitsbehörden

Seit Beginn des Jahres 2007 wird das Gemeinsame Internetzentrum (GIZ) neben dem Gemeinsamen Terrorismusabwehrzentrum – GTAZ – (vgl. 21. TB Nr. 5.1.4) und dem Gemeinsamen Analyse- und Strategiezentrum – GASIM – (vgl. o. Nr. 7.1.5) als ein weiteres behördenübergreifendes Informations- und Kooperationsforum betrieben. Bundesamt für Verfassungsschutz, Bundeskriminalamt, Bundesnachrichtendienst, Militärischer Abschirmdienst und Generalbundesanwalt bündeln hier ihre Kompetenzen, um im Internet nach extremistischen und terroristischen Aktivitäten zu suchen und die Erkenntnisse auszuwerten. Die Tätigkeit der am GIZ beteiligten Behörden war Gegenstand einer datenschutzrechtlichen Kontrolle im Berichtszeitraum (vgl. o. Nr. 4.9).

### 7.1.5 Gemeinsames Analyse- und Strategiezentrum Illegale Migration (GASIM) – Ergebnisse der datenschutzrechtlichen Prüfung

*Bei einem Beratungs- und Kontrollbesuch im Gemeinsamen Analyse- und Strategiezentrum Illegale Migration (GASIM – vgl. 22. TB Nr. 4.2.3) habe ich eine Reihe kritisch zu beurteilender Sachverhalte festgestellt.*

Das GASIM ist ein auf Dauer angelegtes behördenübergreifendes Informations- und Kooperationszentrum mit dem Ziel, die Zusammenarbeit bei der Bekämpfung der illegalen Migration sowie ihrer Begleit- und Folgekriminalität unter Wahrung der spezifischen Rechtsgrundlagen und Zuständigkeiten der an diesem Zentrum beteiligten Kooperationspartner zu intensivieren. Diesem Konzept entsprechend erfolgen in einzelnen Foren Datenübermittlungen und Informationsabfragen zwischen den betroffenen Behörden. Solange dies auf die Zusammenarbeit im strategischen Bereich, d. h. auf den Austausch nicht-personenbezogener Informationen beschränkt bleibt, habe ich keine Einwände. Aus datenschutzrechtlicher Sicht problematisch wird es hingegen, wenn personenbezogene Daten zwischen Kooperationspartnern ausgetauscht und von diesen gemeinsam bewertet werden. Denn am GASIM sind Behörden mit gänzlich unterschiedlichen Aufgaben beteiligt – wie das Bundeskriminalamt, die Bundespolizei, der Bundesnachrichtendienst (BND), aber auch das Bundes-

amt für Migration und Flüchtlinge (BAMF) sowie die Finanzkontrolle Schwarzarbeit (FKS) der Zollverwaltung –, die unterschiedlich weitreichende Befugnisse haben, auch bei der Frage, in welchem Umfang an welche Behörden personenbezogene Daten übermittelt werden dürfen.

So habe ich z. B. festgestellt, dass der BND in dem unter seiner Geschäftsführung tagenden Forum 4 zahlreiche operativ-taktische Hinweise an alle Kooperationsbehörden mit der Bitte um Übermittlung eigener Erkenntnisse zu den Vorgängen bekannt gegeben hatte. Es handelte sich dabei um personenbezogene Erkenntnisse und Informationen, die der BND aus der Beobachtung des Phänomenbereichs „illegale Migration“ im Ausland gewonnen hatte. Problematisch ist dieser Informationsaustausch in Bezug auf das BAMF und die FKS. Aus meiner Sicht sind die insoweit maßgeblichen Übermittlungsvoraussetzungen des § 9 BND-Gesetz mit seinen einschränkenden Zulässigkeitsvoraussetzungen nicht beachtet worden.

Eine ähnliche Problematik stellt sich bezüglich der Zusammenarbeit der Kooperationsbehörden im Forum 7, das sich mit operativen Maßnahmen im Zusammenhang mit der illegalen Migration befasst. Unter der Geschäftsführung der Bundespolizei tauschen hier alle beteiligten Kooperationspartner personenbezogene Daten aus ihrem jeweiligen Zuständigkeitsbereich aus. Auch hier habe ich erhebliche Zweifel, ob die jeweils geltenden Übermittlungsregelungen der Dienstegesetze bzw. des Schwarzarbeitsbekämpfungsgesetzes und des Asylverfahrensgesetzes eine derart dauerhafte und umfassend ausgerichtete Zusammenarbeit, wie mit dem GASIM angestrebt wird, im Einzelfall tragen.

Die Bundesregierung ist meiner Rechtseinschätzung nicht gefolgt. Sie weist darauf hin, dass im GASIM vor allem strategische und damit nicht-personenbezogene Informationen zwischen den beteiligten Kooperationsbehörden ausgetauscht werden. Sofern in einzelnen Fällen personenbezogene Daten übermittelt worden seien, sei dies – mit wenigen Ausnahmen – auf der Grundlage der für die beteiligten Behörden jeweils geltenden bereichsspezifischen Datenverarbeitungsregelungen erfolgt.

Gleichwohl hat die Bundesregierung für die weitere Zusammenarbeit im GASIM insoweit Konsequenzen gezogen, als künftig Sachverhalte, die den Austausch personenbezogener Daten erfordern könnten, institutionalisiert zwischen den beteiligten Behörden stufenweise abgestimmt werden sollen. Ausgehend von einer zunächst abstrakten Sachverhaltsschilderung sollen die Aspekte der Zuständigkeiten bzw. der Aufgabenrelevanz, der Zweckbindung und der Erforderlichkeit vor einer jeden Datenübermittlung geprüft werden. Zudem hat die Bundesregierung die Erstellung von Datenschutzkonzepten der einzelnen im GASIM vertretenen Behörden veranlasst. Weiterhin sollen künftig nur noch flexible, zeitlich begrenzt tätige Arbeitseinheiten projektbezogen betrieben werden.

Ich begrüße diesen Ansatz, scheint er mir doch geeignet, im Rahmen der Tätigkeit des GASIM den unterschiedlichen Kompetenzen und den daran anknüpfenden Datenverarbeitungsbefugnissen der beteiligten Kooperationsbehörden in stärkerem Maße Rechnung zu tragen. Unter den Aspekten der Aufgabenrelevanz und den zur Verfügung stehenden Übermittlungsvorschriften wird zudem die Beteiligung der jeweils betreffenden Behörde erleichtert und dadurch auch mehr Rechtssicherheit für die Tätigkeit des GASIM insgesamt erreicht. Die Entwicklung des GASIM werde ich weiterhin beobachten.

### 7.1.6 Nur der Gesetzgeber bestimmt meine Kontrollkompetenz

*Der Umfang meiner Kontrollkompetenz ist gesetzlich festgelegt. Dies ist mein alleiniger Handlungsmaßstab.*

Alle von mir kontrollierten Stellen sind gesetzlich verpflichtet, mir anlässlich meiner Kontrolle Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren (§ 24 Absatz 4 Nr. 1 BDSG).

Das BfV hat wiederholt (vgl. 18. TB Nr. 14.2; 17. TB Nr. 14.1) gesetzlich nicht verankerte Beschränkungen dieser Kontrollkompetenz geltend gemacht. Die Bedenken des BfV konnten bis jetzt im Rahmen der gesetzlichen Vorgaben immer praxistauglich gelöst werden.

Anlässlich einer Kontrolle hat das BfV nun die Auffassung vertreten, dass ich bei meiner Einsichtnahme in Dateien und Datenverarbeitungsprogramme keine Kenntnis von Namen anderer Nachrichtendienste (sog. AND) nehmen dürfe, die das BfV in diesen Dateien gespeichert habe. Diese Namen unterfielen dem Quellenschutz. Bei meiner Kenntnisnahme bestände die Gefahr negativer Auswirkungen in Bezug auf den Informationsaustausch des BfV mit ausländischen Diensten.

Diese Auffassung widerspricht dem BDSG. Nach dem eindeutigen Gesetzeswortlaut darf meine Kontrollkompetenz nur ausnahmsweise und im Einzelfall beschränkt werden. Dies ist der Fall, wenn die für die kontrollierte Stelle zuständige oberste Bundesbehörde im Einzelfall feststellt, die Auskunft der kontrollierten Stelle oder meine Einsichtnahme in deren Dateien oder Datenverarbeitungsprogramme gefährde die Sicherheit des Bundes oder eines Landes (vgl. § 24 Absatz 4 Satz 4 BDSG), etwa wenn durch meine Einsichtnahme Leib oder Leben einer menschlichen Quelle gefährdet wäre. Dann hätte die konkrete Gefahr für Leib oder Leben der Quelle Vorrang vor meiner Kontrollkompetenz.

Der Schutz der Namen der AND rechtfertigt nicht eine derartige Beschränkung, zumal mir sonst aufgrund der Vielzahl derartiger Dateispeicherungen die mir gesetzlich obliegende Einsicht in Dateien unmöglich wäre.

Als Kompromissvorschlag habe ich dem BfV angeboten, vor meiner Einsichtnahme in eine Datei die dort gespeicherten Namen der AND zunächst technisch auszublenden bzw. unkenntlich zu machen. Das BfV sieht insoweit noch Klärungsbedarf. Ich bin weiterhin zu einer praxistauglichen Lösung bereit, die den gesetzlichen Vorgaben

entspricht. Bei Redaktionsschluss dauerten die Beratungen an.

### 7.1.7 Polizeiliche Ermittlungen in sozialen Netzwerken

*Ermittlungen im Internet haben breiten Einzug in die polizeiliche Arbeit gefunden (vgl. 18. TB Nr. 11.8; 21. TB Nr. 5.1.3). Dabei wird zunehmend auch in sozialen Netzwerken recherchiert.*

Auch das BKA nutzt soziale Netzwerke (vgl. o. Nr. 4.5) und andere open sources für Abklärungen im Rahmen von Ermittlungsverfahren und zur Erfüllung seiner Zentralstellenaufgabe gem. § 2 BKA-Gesetz. Zweck sei es, die Begehung konkreter Straftaten zu erkennen und diese den sachlich und örtlich zuständigen Strafverfolgungsbehörden mitzuteilen. Unter Bezug auf das Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 zur sog. Online-Durchsuchung (BVerfG 1 BvR 370/07 – vgl. auch 22. TB Nr. 4.1.1) hebt das BKA hervor, die reine Internetaufklärung stelle in aller Regel keinen Grundrechtseingriff dar. Sollten derartige Recherchen in sozialen Netzwerken in einzelnen Fällen Eingriffsqualität haben, würden als Befugnisnormen §§ 161, 163 StPO oder § 7 Absatz 1 und 2 BKA-Gesetz greifen.

Hier stellt sich dieselbe Problematik wie bei der Tätigkeit der am Gemeinsamen Internetzentrum (GIZ) beteiligten Behörden (vgl. o. Nr. 4.9). Maßgebend ist, in welchem Stadium der polizeilichen Internet-Recherche das schutzwürdige Vertrauen des Betroffenen in die Identität seines Kommunikationspartners ausgenutzt wird. Unbeschadet dessen liegt aber nach der Rechtsprechung des Bundesverfassungsgerichts (a. a. O.) ein Eingriff in das Recht auf informationelle Selbstbestimmung immer dann vor, wenn die im Internet erhobenen Daten gezielt zusammengetragen, gespeichert und ausgewertet werden. Dies ist der Fall, wenn das BKA im Rahmen strafrechtlicher Ermittlungsverfahren oder zu Auswertezwecken im Rahmen seiner Zentralstellenaufgabe in sozialen Netzwerken recherchiert.

Ich habe Zweifel, inwieweit die vom BKA angeführten Rechtsnormen den Eingriff in das informationelle Selbstbestimmungsrecht bei Ermittlungen in sozialen Netzwerken legitimieren können. Nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 bedürfen Einschränkungen dieses Grundrechts einer normenklaren gesetzlichen Grundlage, die Voraussetzung und Umfang der Beschränkungen klar und für den Betroffenen erkennbar regelt. Die generalklauselartigen Befugnisnormen der §§ 161, 163 StPO bzw. § 7 Absatz 1 und 2 BKA-Gesetz erfüllen diese Voraussetzungen nicht. Auch im Hinblick auf die nicht nur von mir empfundene Rechtsunsicherheit, in welchem Stadium der polizeilichen Recherchen im Internet von einem Eingriff in Grundrechte auszugehen ist, halte ich es für geboten, Inhalt und Grenzen derartiger Befugnisse spezialgesetzlich zu regeln.

## 7.2 Bundeskriminalamt

Schwerpunkte meiner Tätigkeit im Berichtszeitraum waren die Begleitung der Arbeiten an der Rechtsverordnung gem. § 7 Absatz 6 BKAG (vgl. u. Nr. 7.2.1), die datenschutzrechtliche Prüfung der Datenverarbeitung durch das BKA in den Staatsschutzdateien (vgl. u. Nr. 7.2.2) sowie deren Beteiligung an Zuverlässigkeitsüberprüfungen im Rahmen von Akkreditierungen bei Großveranstaltungen (vgl. u. Nr. 7.2.3).

### 7.2.1 Mit viel Verspätung: eine Rechtsverordnung über die Arten von Daten, die das BKA als Zentralstelle speichern darf

*Das BMI hat im vergangenen Sommer einen abschließenden Katalog von Datenarten festgelegt, die das BKA in seiner Funktion als Zentralstelle speichern darf. Damit kommt das BMI einer von mir seit Langem erhobenen Forderung nach – allerdings nur nach gerichtlichem Druck.*

In meinen letzten Tätigkeitsberichten hieß es wiederholt: „Noch immer keine Rechtsverordnung gemäß § 7 Absatz 6 BKAG“ (vgl. 22. TB Nr. 4.3.2.3). Dies hat sich nun geändert: Seit dem 9. Juni 2010 ist die „Verordnung über die Art der Daten, die nach den §§ 8 und 9 des Bundeskriminalamtgesetzes gespeichert werden dürfen“ in Kraft, die nun abschließend regelt, welche Arten von Daten das BKA in seiner Funktion als Zentralstelle in Dateien speichern darf (BGBl. I S. 716). Zu diesem Katalog gehören weniger kritische Datenarten wie Name oder Geburtsort, aber auch sensiblere Angaben, wie etwa Religionszugehörigkeit, Kontoverbindung, Bestand in der DNA-Analyse-Datei oder ein Hinweis wie „Straftäter links motiviert“.

Den Erlass einer solchen Rechtsverordnung habe ich schon seit Jahren gefordert; zuletzt in einer gemeinsamen Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. März 2009 (vgl. Kasten zu Nr. 7.2.1). Das BKAG enthält nämlich eine Pflicht zum Erlass einer solchen Verordnung – und das aus gutem Grund: Nur so bestimmt auch der Bundesrat mit, welche Daten das BKA als Zentralstelle speichern darf. Und nur so entsteht die gebotene Transparenz.

Nachdem sich das BMI diesen Argumenten jahrelang verschlossen hatte, zwang es ein Urteil des OVG Lüneburg, seine Position zu überdenken. Das niedersächsische OVG hatte nämlich die Speicherung von Daten in der gemeinsam von Bund und Ländern geführten Datei „Gewalttäter Sport“ – also der sogenannten „Hooligan“-Datei – aufgrund der fehlenden Rechtsverordnung für rechtswidrig erklärt (Urteil vom 16. Dezember 2008, 11 LC 228/08). Damit stand allerdings zugleich ein großer Teil der Datenverarbeitung im BKA mit auf dem Spiel. Denn wenn eine Rechtsgrundlage nach § 7 Absatz 6 BKAG konstitutiv ist, wie das OVG befand, gilt dies auch für alle anderen Dateien, die das BKA als Zentralstelle führt. Ohne Rechtsverordnung waren diese sämtlich in Gefahr, rechtswidrig zu sein.

Dies hat das BMI gerade noch vermeiden können. Denn die Rechtsverordnung trat just an dem Tag in Kraft, an dem das Bundesverwaltungsgericht über die Revision in dem oben genannten Fall entschieden hat. Zwar hat das Bundesverwaltungsgericht die streitige Speicherung in der Datei „Gewalttäter Sport“ deshalb für rechtmäßig befunden, es ließ aber keinen Zweifel daran, dass es die Rechtsauffassung des OVG bestätigt hätte. Bei § 7 Absatz 6 BKAG handele es sich nicht um eine „bloße Verordnungsermächtigung, sondern um einen strikten Regelungsauftrag“ (Urteil vom 9. Juni 2010, 6 C 5.09).

Kasten zu Nr. 7.2.1

**Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. März 2009 in Berlin**

**Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage**

Die Speicherung von Daten im polizeilichen Informationssystem INPOL durch die Polizeien des Bundes und der Länder ist nur dann rechtmäßig, wenn eine Rechtsverordnung gemäß § 7 Absatz 6 Bundeskriminalamtsgesetz das Nähere über die Art der Daten bestimmt, die in dieser Datei gespeichert werden dürfen. Eine solche Rechtsverordnung existiert nicht. Mit Urteil vom 16. Dezember 2008 (Az. 11 LC 229/08) hat das Niedersächsische Oberverwaltungsgericht dies in Bezug auf die Verbunddatei „Gewalttäter Sport“ bekräftigt. Das Urteil ist nicht nur für die Rechtmäßigkeit der Hooligan-Datei bedeutsam, sondern hat Auswirkung auf alle im Rahmen von INPOL geführten Verbunddateien.

Mit der Entscheidung des Gerichts wird die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt. Die vom Bundesministerium des Innern bisher vertretene Auffassung, wonach die Rechtsverordnung keine Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien sei, wird durch die einschlägigen Regelungen nicht gestützt.

Ohne eine derartige Rechtsverordnung ist die Gesamtheit der in Verbunddateien stattfindenden polizeilichen Datenverarbeitungen rechtswidrig. Die Datenschutzbeauftragten von Bund und Länder fordern das Bundesministerium des Innern und die Landesregierungen auf, unverzüglich daraus Konsequenzen zu ziehen und die polizeiliche Datenverarbeitung auf den Prüfstand zu stellen.

Die neu geschaffene Rechtsverordnung ist keine Rechtsgrundlage für die Erhebung oder Verarbeitung von Daten. Es ging nicht darum, mehr Daten oder neue Arten von Daten zu erfassen, sondern die Speicherung der vorhandenen Daten auf rechtstaatliche Grundlagen zu stellen. Im Verfahren habe ich erfolgreich darauf gedrungen, dass die Arten von Daten in der Rechtsverordnung abschließend aufgeführt sind. Andere Daten darf damit das BKA in seine Dateien nicht aufnehmen.

Zugleich bestand während der Ressortberatungen Übereinstimmung darin, dass die Rechtsverordnung nicht einfach nur eine einzige lange Liste von Datenarten sein dürfe, sondern diese den verschiedenen Arten von Dateien zuordnen müsse. Dieses Konzept ist auch durchgehalten worden, was allerdings zu einem äußerst komplexen Verordnungstext geführt hat.

Leider wurde die Chance vertan, die zu speichernden Datenarten auf das erforderliche Maß zu beschränken. Mit den Verordnungsregelungen wurde der durch die §§ 8, 9 BKA-Gesetz gesteckte gesetzliche Rahmen vollständig ausgeschöpft. So bin ich mit meiner Forderung, den Satz an „Grunddaten“ zu erfassten Personen zu beschränken, nicht durchgedrungen. Meine Anregung, in dem Verordnungstext die Regelung des § 8 Absatz 5 BKAG zu „sonstigen Personen“ weiter zu konkretisieren, ist ebenso nicht aufgegriffen worden.

### 7.2.2 Politisch motivierte Kriminalität – Die Datei „IgaSt“ beim BKA

*Gegen die Speicherpraxis des BKA in der Datei „IgaSt“, aus der Listen im Vorfeld von globalisierungskritischen Demonstrationen ins Ausland versendet werden, bestehen Bedenken.*

Im Zusammenhang mit politischen Großveranstaltungen, wie etwa dem NATO-Gipfel in Straßburg und Kehl oder der Weltklimakonferenz in Kopenhagen, ist es üblich geworden, zwischen den Sicherheitsbehörden Informationen zu potentiell gewalttätigen Demonstranten über die Landesgrenzen hinaus auszutauschen. Die Antworten der Bundesregierung auf Anfragen von Abgeordneten zu diesem Thema ließen allerdings einige Frage bei mir offen. Deswegen habe ich die Datenverarbeitungspraxis des BKA im Bereich der sog. politisch motivierten Kriminalität kontrolliert. Im Zentrum stand dabei die Datei „International agierende gewaltbereite Störer – IgaSt“, die der mittlerweile gelöschten Datei „Global“ (vgl. 20. TB Nr. 5.2.5.1) nachgefolgt ist.

Die Datei „IgaSt“ hat ein gewisses Maß an Bekanntheit erlangt, weil sie Grundlage für eine Liste von „gewaltbereiten Störern“ mit globalisierungskritischer Haltung ist. Das BKA versendet diese an die Polizei des Veranstalterlandes, sofern mit Ausschreitungen gerechnet wird. Dem Empfänger wird dabei vorgegeben, spätestens vier Wochen nach dem Ende des Ereignisses die mitgeteilten Daten zu löschen. Jede Übermittlung personenbezogener Daten in diesem Zusammenhang erfolgt zudem mit einer Datenschutzklausel, die u. a. die Zweckbindung der übermittelten Daten festschreibt. Zudem wird die Datenübermittlung vom Vorliegen eines angemessenen Datenschutzniveaus im Empfängerland abhängig gemacht.

Es ist aber nicht diese Praxis der Datenübermittlung, die auf meine datenschutzrechtlichen Bedenken gestoßen ist, sondern vielmehr die Struktur der Datei „IgaSt“ und die Art und Weise ihrer Führung:

Die in der Datei gespeicherten Personen werden in zwei Kategorien eingeteilt, ohne dass dies aus der mir vorliegenden Errichtungsanordnung hervorgeht. Während in der einen Kategorie die Personen erfasst sind, die dem

„harten Kern“ der gewaltbereiten Störer zugerechnet und im Bedarfsfall in die o. g. Liste aufgenommen werden, erfolgt die Speicherung der übrigen Personen zunächst nur, um zu einem späteren Zeitpunkt zu entscheiden, ob sie im Laufe der Speicherfrist auf die Liste zu nehmen oder in der Datei zu löschen sind. Die Datei enthält damit Beschuldigte, Verdächtige oder sog. sonstige Personen im Sinne von § 8 BKA-Gesetz, entgegen ihrer Errichtungsanordnung aber keine sog. tatfernen Personen, wie z. B. Zeugen oder Kontaktpersonen. Zudem werden auch die o. g. Umstände der Datenübermittlung in der Errichtungsanordnung nicht festgelegt. Die Errichtungsanordnung erfüllt damit nicht die vom Gesetzgeber zugewiesene konkretisierende Funktion.

Ich habe auch nicht den Eindruck gewonnen, dass hinreichend klar bestimmt ist, bei wem es sich nach Auffassung des BKA um einen „international agierenden gewaltbereiten Störer“ handelt, insbesondere in den Fällen, in denen die betreffende Person zwar in der Datei gespeichert, aber nicht dem „harten Kern“ gewaltbereiter Störer zugerechnet wird. Auch die Faktenbasis, auf der das BKA seine Prognoseentscheidung treffen muss, erschien mir häufig unsicher, zumal das BKA hier auf teilweise sehr lückenhafte Informationen aus dem Ausland bzw. aus den Ländern angewiesen ist. Gleichwohl trägt das BKA die datenschutzrechtliche Verantwortung für die Speicherungen in der Datei „IgaSt“. Wie ich dem BKA gegenüber zum Ausdruck gebracht habe, halte ich bestimmte Speicherungen nicht für gerechtfertigt. Das gilt z. B. für Fälle, in denen Demonstranten erfasst wurden, die in einer Menschenkette oder als Teil des „nackten Blocks“ Straßenblockaden durchgeführt hatten. Ungeachtet der juristischen Frage, inwieweit die Handlungen von Demonstranten strafrechtlich unter den umstrittenen Begriff der „Gewalt“ subsumiert werden können, sollte eine Speicherung in der Datei nur dann erfolgen, wenn die gewählte Form des politischen Protests zu erkennen gibt, dass Menschen verletzt oder Sachwerte in nicht unerheblichem Umfang zerstört werden sollen. Nur so kann sichergestellt werden, dass auch provokante Formen des politischen Protests zulässig bleiben. Auch wenn in diesen Fällen die Namen der Betroffenen nicht ins Ausland übermittelt wurden, führt allein die Speicherung in der Datei „IgaSt“ zu einem Eingriff in das informationelle Selbstbestimmungsrecht.

Das BKA hat zugesagt, die Speicherpraxis zu überprüfen. Eine Stellungnahme lag bis Redaktionsschluss noch nicht vor.

### 7.2.3 Beteiligung des BKA an Zuverlässigkeitsüberprüfungen

*Was anlässlich der Fußball-WM 2006 noch als singuläre Maßnahme deklariert worden war (vgl. 21. TB Nr. 5.2.5), hat sich mittlerweile bei den Sicherheitsbehörden als Standardinstrument etabliert: die einwilligungsbasierte Zuverlässigkeitsüberprüfung von zu akkreditierenden Personen bei Großveranstaltungen. Hier ist gesetzgeberisches Handeln dringend angesagt.*

Auch im Berichtszeitraum waren das BKA und andere Sicherheitsbehörden bei Großveranstaltungen an Zuverlässigkeitsüberprüfungen von zu akkreditierenden Personen beteiligt, so u. a. beim NATO-Gipfel 2009 in Straßburg und Kehl oder im Vorfeld der Ski-WM 2011 in Deutschland. Als Grundlage hierfür diente jeweils die Einwilligung der Betroffenen, zumeist Medienvertreter. Das Verfahren läuft dabei nach dem immer gleichen Muster ab: Die personenbezogenen Daten derer, die eine Akkreditierung für die Großveranstaltung beantragen, werden vom Veranstalter u. a. an das BKA übermittelt, um festzustellen, ob sicherheitsrelevante Erkenntnisse zu den jeweiligen Personen vorliegen. Dort werden die Daten mit bestimmten Dateien des polizeilichen Informationssystems INPOL sowie mit BKA-eigenen Dateien abgeglichen. Das Ergebnis wird dem Veranstalter zurückgemeldet.

Die Einwilligung vermag die Datenverarbeitung bei den Sicherheitsbehörden im Zusammenhang mit den Zuverlässigkeitsüberprüfungsverfahren nicht zu legitimieren. Es fehlt bereits an der für ihre Wirksamkeit nach dem Bundesdatenschutzgesetz erforderlichen Freiwilligkeit. Die Akkreditierungsbewerber geben die Einwilligung nur deshalb ab, weil sie andernfalls Nachteile befürchten, u. a. ihrem Beruf nicht nachgehen zu können. Die Betroffenen werden zudem nicht umfassend über die beabsichtigte Verarbeitung und Verwendung ihrer Daten unterrichtet. So wird in einem Fall in der der Einwilligung zugrundeliegenden Datenschutzinformation nur beispielhaft auf die Dateien hingewiesen, die in den beabsichtigten Datenabgleich einbezogen werden sollen. In einem anderen Fall fehlt der Hinweis, an wen das Ergebnis des Datenabgleichs übermittelt wird. Letzteres hatte auch das Verwaltungsgericht Wiesbaden in seinem Urteil vom 6. Oktober 2010 (6 K 280/10.WI) bemängelt. Das Gericht hielt die Abgabe eines Votums des BKA durch Übermittlung personenbezogener Daten eines Akkreditierungsbewerbers an die NATO im Verfahren der Erteilung einer Presseakkreditierung für den NATO-Gipfel 2009 für rechtswidrig.

Zuverlässigkeitsüberprüfungen greifen tief in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe bedürfen aber einer normenklaren Rechtsgrundlage, die die Voraussetzungen und Begrenzungen eines solchen Verfahrens regelt. Hierauf hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 25./26. Oktober 2007 hingewiesen (vgl. 22. TB Nr. 4.8.3.2).

Da die Sicherheitsbehörden auf das Instrument der Zuverlässigkeitsüberprüfung bei Großveranstaltungen nicht verzichten wollen, gleichzeitig das praktizierte Verfahren aber erhebliche Defizite aufweist, ist gesetzgeberisches Handeln dringend angeraten.

## 7.3 Bundespolizei

Im Berichtszeitraum standen Fragen des technologischen Datenschutzes im Vordergrund meiner Tätigkeit: Die Beteiligung an der Diskussion über die Einführung von Körperscannern an Flughäfen und das dazu von der Bundespolizei durchgeführte Forschungsvorhaben (vgl. u. Nr. 7.3.1), die Begleitung des Pilotprojektes „Biometrisches

Grenzkontrollverfahren easyPass“ (vgl. u. Nr. 7.3.2) sowie die Einführung der elektronischen Kriminalakte bei der Bundespolizei (vgl. u. Nr. 7.3.3).

### 7.3.1 Körperscanner auf deutschen Flughäfen – Fortschritte und Probleme

*Erstmalig werden auf einem deutschen Flughafen Körperscanner erprobt. Dabei sind offensichtlich meine Forderungen nach einem weitgehenden Schutz der Persönlichkeitsrechte bisher berücksichtigt worden.*

Bei vielen Maßnahmen, die gegen terroristische und kriminelle Gefahren gefordert werden, steht der Datenschutz – aber nicht nur er – vor einem Dilemma: In welchem Maße darf in Persönlichkeitsrechte eingegriffen werden, um den beschriebenen Gefahren zu begegnen oder zumindest die Risiken zu minimieren? Vielfach geht es dabei um die Auswahl zwischen Alternativen, die jede für sich bedenkliche Konsequenzen haben könnte. In besonderem Maße gilt dies für die Sicherheit im Flugverkehr, der bereits wiederholt Ziel terroristischer Aktionen war.

Nach dem gescheiterten Anschlagsversuch auf ein Flugzeug auf dem Weg nach Detroit an Weihnachten 2009 entfaltete sich auch in Deutschland eine intensive Diskussion über Sinn und Risiko der Einführung von Körperscannern auf deutschen Flughäfen. Mich erreichten hierzu auch viele E-Mails von Bürgerinnen und Bürgern mit ganz unterschiedlichem Inhalt. Während einige wenig Verständnis für datenschutzrechtliche Bedenken zeigten, äußerten viele andere ihre Sorgen um den Schutz ihrer Persönlichkeitsrechte. Sie fürchteten eine Verletzung ihres Schamgefühls, eine Bloßstellung durch eine neue Form der Durchleuchtung, die ihre jeweiligen Leiden oder Besonderheiten, wenn nicht öffentlich, so doch für Fremde sichtbar machten; zumal damals auch noch Bilder von Körperscannern in den Medien kursierten, die von echten „Nacktscannern“ gemacht wurden.

Um die öffentliche Debatte über mehr Sicherheit zu versachlichen und gleichzeitig klar zu machen, welche Grenzen beim Ruf nach mehr Sicherheit nicht überschritten werden dürfen, habe ich datenschutzrechtliche Voraussetzungen formuliert, ohne deren Erfüllung die Einführung von Körperscannern nicht in Betracht kommen darf. In diesem Sinne habe ich gemeinsam mit den Datenschutzbeauftragten der Länder während der 79. Datenschutzkonferenz am 17./18. März 2010 eine Entschließung verfasst (vgl. Kasten zu Nr. 7.3.1.).

Danach gilt: Keine Körperscanner ohne den Nachweis eines Sicherheitsgewinns, keine Speicherung der erhobenen Daten und optimaler Schutz der Menschenwürde, indem keine menschlichen Konturen, keine Geschlechtsmerkmale oder medizinische Hilfsmitteln (wie etwa Windeln oder künstliche Darmausgänge) auf dem Bildschirm als solche sichtbar gemacht werden.

Gemessen daran halte ich die Geräte, wie sie gegenwärtig vom zuständigen BMI auf dem Flughafen Hamburg erprobt werden, für deutlich besser als die Vorgängermodelle, insbesondere weil jede überprüfte Person nicht in ihren wirklichen Körperformen sondern als ein unpersönliches Strichmännchen dargestellt wird. Ich sehe allerdings noch weiteren Verbesserungsbedarf. So habe ich gegenüber dem BMI angeregt, die eingesetzten Körperscanner nach anerkannten Maßstäben (sog. common criteria) durch unabhängige Sachverständige zertifizieren zu lassen. Ich erwarte von der Bundesregierung außerdem, dass sie sich auch auf europäischer Ebene für die von ihr akzeptierten Voraussetzungen als europaweite Mindeststandards einsetzt. Zudem ist nach den bisherigen Erkenntnissen die Fehlerquote der Geräte noch sehr hoch, so dass der Nachweis eines Sicherheitsgewinns und der Einsatztauglichkeit noch aussteht.

Kasten zu Nr. 7.3.1

**Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010**

**Körperscanner – viele offene Fragen**

Der Anschlagsversuch von Detroit am 25. Dezember 2009 hat die Diskussion über den Einsatz von sog. Körperscannern bei der Passagierkontrolle am Flughafen neu entfacht. Mit dieser Technik sollen Sicherheitslücken geschlossen werden. Es ist aber noch weitgehend unklar, was diese Geräte technisch leisten können und wie sie sich in ein konsistentes Gesamtsystem zur Flugsicherheit einfügen lassen. Eine Entscheidung über den Einsatz solcher Geräte, die der Gesetzgeber zu treffen hätte, setzt zumindest die Erfüllung folgender Bedingungen voraus:

1. Es muss geklärt werden, ob mit diesen Geräten ein nennenswerter Sicherheitsgewinn erzielbar ist. Derzeit bestehen zumindest ernsthafte Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie, vor allem im Hinblick auf die Detektierbarkeit von Materialien mit geringer Dichte, etwa pulverförmigen Substanzen, wie sie im Fall des Anschlagsversuchs von Detroit verwendet worden sind.
2. Es muss sichergestellt sein, dass die beim Einsatz der Körperscanner erhobenen Daten der Kontrollierten über den Scanvorgang hinaus nicht gespeichert werden. Auch die Anzeige der Körperkonturen gegenüber dem Kontrollpersonal und die Speicherung der erstellten Bilder über den Scanvorgang hinaus sind technisch auszuschließen.
3. Selbst wenn die vorstehenden Bedingungen erfüllt werden, darf der Einsatz von Scannern die Grundrechte der Betroffenen, insbesondere die absolut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzen. So dürften z. B. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel (etwa Prothesen und künstliche Darmausgänge) nicht angezeigt werden. Gesundheitsschäden sind auszuschließen.
4. Die Erfüllung dieser Bedingungen ist in praktischen Tests und Erprobungen nachzuweisen.

Nachdem ich die eingesetzten Geräte schon vor Beginn der Erprobung auf dem Hamburger Flughafen im Forschungslabor der Bundespolizei in Augenschein genommen habe, werde ich auch den weiteren Testverlauf des Körperscanners sehr genau beobachten. Dabei werde ich bei einer anstehenden Kontrolle in erster Linie darauf achten, dass keinerlei Daten gespeichert werden und die Nachuntersuchungen in erforderlichen Diskretionszonen und mit der erforderlichen Sensibilität durch das Kontrollpersonal vorgenommen werden. Denn eines lässt sich wohl nicht vermeiden: Wenn die Körperscanner so eingestellt sind, dass sie mehr gefährliche Gegenstände detektieren können, dann sind sie auch so eingestellt, dass sie auch vieles detektieren, was nicht gefährlich ist.

### 7.3.2 Biometrische Grenzkontrollverfahren an Flughäfen – Auf dem Weg zur Sortierung von Flugreisenden nach Risikokategorien?

*Der internationale Airline-Verband IATA hat eine grundlegende Änderung des Systems der Sicherheitskontrollen auf Flughäfen vorgeschlagen, das auf einer Sortierung der Flugreisenden nach Risikokategorien basiert.*

Zunächst sollen die Passagiere mittels biometrischer Merkmale identifiziert werden. Auf dieser Basis findet ein Abgleich mit den Buchungsdaten statt. In einem weiteren Schritt werden die Reisenden in drei Kategorien eingeteilt: bekannte Flugreisende, normale Flugreisende und potentielle Gefährder. Je nach Ergebnis der Risikoabschätzung sollen die Passagiere dann in drei „Tunneln“ einer differenzierten Sicherheitskontrolle unterworfen werden. Während die „bekannten Reisenden“ – im Wesentlichen dürfte es sich dabei um Geschäftsreisende handeln – einer eher oberflächlichen physischen Kontrolle unterzogen werden, ist anzunehmen, dass die anderen Kategorien schärfer kontrolliert werden, wobei insbesondere die „potentiellen Gefährder“ besonders scharf durchsucht und befragt werden.

Nach meiner Auffassung ist eine solche Kategorisierung jedoch inakzeptabel.

Die Einstufung der Passagiere erfolgt nach völlig undurchsichtigen Kriterien. Voraussichtlich werden von dieser Regelung nur Businessreisende profitieren. Für die „Normal“-Reisenden ergeben sich im Regelfall keine Verbesserungen. Passagiere die das „Pech“ haben, als „potentielle Gefährder“ eingestuft zu werden, wären durch das IATA-Modell sogar von umfangreicheren, langwierigeren und tiefer gehenden Kontrollen betroffen. Da kein „normaler“ Passagier seine Einsortierung vorhersehen kann, müssten wohl alle „Wenigflieger“ früher als derzeit üblich am Flughafen erscheinen, um auch eine Prüfung als „potentieller Gefährder“ noch rechtzeitig durchlaufen zu können. Zudem sehe ich den damit verbundenen umfassenden Datenabgleich aller Reisenden kritisch, weil nicht nur Daten, die für völlig andere Zwecke erhoben worden sind, für eine Risikobewertung verwendet, sondern auch weitere Daten staatlicher Stellen sowie zusätzliche Verhaltenskontrollen auf Basis von individuellen Interviews zur Risikobewertung einbezogen werden. Dieser Datenabgleich würde kombiniert mit einem System individueller Ausforschung. Ich halte den diskriminierenden Effekt eines solchen Systems für beträchtlich und deswegen den IATA-Vorschlag für fragwürdig. Seine Verwirklichung wäre nichts anderes als eine weitere Drehung der Sicherheitsschraube zulasten der Persönlichkeitsrechte.

Auch die von der Bundespolizei betriebenen biometrischen Grenzkontrollverfahren „Automatisierte und biometriegestützte Grenzkontrolle-ABG“ (vgl. 20. TB Nr. 5.3.5; 21. TB Nr. 4.5.2) und „EasyPASS“ (s. o. Nr. 3.5; 22 TB Nr. 6.4) sind vor diesem Hintergrund zu betrachten, dienen sie doch gerade dazu, Flugpassagiere anhand biometrischer Daten zu identifizieren. Sie würden damit einen Baustein des von IATA propagierten Sicherheitskontrollsystems darstellen.

### 7.3.3 Bundespolizei führt die elektronische Kriminalakte ein

*Die Bundespolizei stellt gegenwärtig ihre Kriminalaktenhaltung auf eine elektronische Form um. Damit sind auch datenschutzrechtliche Risiken verbunden.*

Im Berichtszeitraum hat mich die Bundespolizei über ihre Entscheidung informiert, die herkömmlich in Papierform geführte Kriminalakte weitestgehend durch eine elektronische Kriminalakte (eKA) zu ersetzen.

Diese Umstellung der Kriminalaktenhaltung wirft grundlegende datenschutzrechtliche Fragen auf. Denn je nach Ausgestaltung kann dies insbesondere dazu führen, dass mehr Daten gespeichert, Daten doppelt oder mehrfach vorgehalten und der Zugriff auf die Daten bzw. die Recherchemöglichkeiten unangemessen ausgeweitet werden. So ist geplant, den Umfang der Maßnahmen und damit einhergehend den Kreis der Personen, die in der eKA erfasst werden, weit zu ziehen – von Maßnahmen der Strafverfolgung und Gefahrenabwehr bis hin zu den der Bundespolizei nach anderen Gesetzen zugewiesenen Aufgaben. Außerdem ist vorgesehen, dass die Dienststellen der Bundespolizei auf den gesamten Bestand der eKA Zugriff erhalten. Mit den Verfahren „@rtus“ (vgl. 21. TB Nr. 5.3.1) und „Bundespolizeiaktennachweis“ (vgl. 20. TB Nr. 5.3.2) werden zudem Dateien bei der Bundespolizei betrieben, deren Aufgaben und Zwecke sich zum Teil mit denen der eKA überschneiden. Dies kann zu Mehrfachspeicherungen personenbezogener Daten führen. Die Ausgestaltung der elektronischen Kriminalakte macht es daher erforderlich, darüber nachzudenken, ob andere Datenbestände hinfällig werden und damit gelöscht werden können und wie Missbrauch vermieden werden kann, wenn nun sehr viel mehr Bundespolizisten mit einem Mausklick und einigen zusätzlichen Angaben Zugriff auf fast alle in der elektronischen Kriminalakte enthaltenen Daten erhalten. Daneben stellen sich auch bei der elektronischen Kriminalakte schon bekannte Fragen, etwa danach, wie der Kreis der erfassten Personen auf das Erforderliche begrenzt werden kann und nach welchem Zeitablauf eine Überprüfung der Speicherung vorgenommen werden sollte. Ein besonderer Mehrwert der elektronischen Kriminalakte wird von der Bundespolizei zudem darin gesehen, dass die neue Datei

ein Eingabefeld zu Informationen über die Persönlichkeit des Betroffenen enthält.

Nach einem ersten Vorgespräch habe ich noch während der Pilotphase zur Einführung der elektronischen Kriminalakte einen Kontroll- und Beratungsbesuch bei der Bundespolizeidirektion Flughafen Frankfurt/Main durchgeführt. Bis zum Redaktionsschluss war die Bewertung des umfangreichen Materials noch nicht abgeschlossen. Ich werde diese Thematik in meinem nächsten Tätigkeitsbericht erneut aufgreifen und von den Ergebnissen der Kontrolle berichten.

### 7.4 Präventive Telekommunikationsüberwachung und „Quellen-TKÜ“ beim Zollkriminalamt

*Das Zollkriminalamt verfügt über die Befugnis zur präventiven Telekommunikationsüberwachung. Daneben nimmt es auch „Quellen-TKÜ“ vor, dringt also im Rahmen von Telekommunikationsüberwachungen in Computersysteme ein, um auch verschlüsselte Gespräche abzuhören.*

Gegen Ende des Berichtszeitraums habe ich einen Beratungs- und Kontrollbesuch im Zollkriminalamt (ZKA) durchgeführt, um zu prüfen, wie das ZKA von der präventiven Telekommunikationsüberwachung (TKÜ) Gebrauch macht, also der Überwachung von E-Mails und Telefongesprächen, ohne dass im Zeitpunkt der Beantragung der Überwachung ein Strafverfahren gegen die überwachte Person eröffnet ist. Die Befugnis für diesen tiefen und zeitlich früh ansetzenden Grundrechtseingriff ist vor Jahren in das Zollfahndungsdienstgesetz (ZFdG) eingefügt worden, um der Zollfahndung ein weiteres Mittel zur Verhinderung illegaler Ausfuhren und zur Unterbindung von drohenden Verstößen gegen das Kriegswaffenkontrollgesetz zur Verfügung zu stellen (vg. 21. TB Nr. 5.4.1).

Bei der Kontrolle zeigte sich, wie stark sowohl die Praxis der Erhebung als auch die der Verarbeitung der präventiv erhobenen Telekommunikationsdaten durch die Gerichte bestimmt wird. Dies betrifft nicht nur den in aller Regel erforderlichen Antrag bei Gericht vor Durchführung einer solchen Maßnahme, sondern ebenso die Speicherungspraxis bzgl. der dabei gewonnenen Daten. So wird auch das gesetzlich vorgesehene Verfahren der Benachrichtigung der von einer Überwachungsmaßnahme Betroffenen wesentlich durch die gerichtliche Spruchpraxis geprägt, bedarf doch das Aufschieben der Benachrichtigung bzw. das gänzliche Absehen davon jeweils der gerichtlichen Zustimmung. Meine Kontrolle habe ich daher u. a. auf die Frage fokussiert, wie das ZKA mit Inhalten umgeht, die den sogenannten Kernbereich privater Lebensgestaltung betreffen.

Durch einen Zeitungsbericht habe ich zudem erfahren, dass das ZKA schon verschiedentlich „Quellen-TKÜ“ durchgeführt hat. Hinter diesem Begriff verbirgt sich die Überwachung von Gesprächen, deren Inhalte nur in verschlüsselter Form übertragen werden. Das bekannteste Beispiel hierfür ist die Internet-Telefonie. Um derartige Gespräche abzuhören, ist es erforderlich, ein Programm auf einem der an der Kommunikation beteiligten Rechner aufzuspielen, das schon vor der Verschlüsselung einen Zugriff auf die Daten ermöglicht. Damit ähnelt die Maßnahme in ihrer technischen Ausführung der „Online-Durchsuchung“. In Abgrenzung dazu muss bei einer „Quellen-TKÜ“ technisch sichergestellt sein, dass der Zugriff ausschließlich auf Daten einer laufenden Telekommunikation erfolgt. Andere auf dem Computer gespeicherte Daten dürfen dabei nicht erhoben werden. Sehr umstritten ist die Frage, auf welcher Rechtsgrundlage eine „Quellen-TKÜ“ vorgenommen werden darf. Nach meiner Auffassung kann diese Maßnahme nicht auf die Rechtsgrundlage für eine herkömmliche Telekommunikationsüberwachung, wie etwa § 100a StPO oder eben auch § 23a ZFdG, gestützt werden. Im Anschluss an das Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 zur sog. Online-Durchsuchung (1 BvR 370/07 – vgl. 22. TB Nr. 4.1.1) halte ich eine gesonderte gesetzliche Befugnis für erforderlich, wie sie in § 20l BKA-Gesetz geschaffen wurde.

Bis Redaktionsschluss habe ich die im Rahmen der Kontrolle gewonnenen Erkenntnisse noch nicht abschließend bewerten können. Insbesondere wird es noch erforderlich sein, über die rechtliche Kontrolle der präventiven TKÜ hinaus auch aus technischer Sicht nachzuvollziehen und zu kontrollieren, wie das ZKA die für die Durchführung der „Quellen-TKÜ“ erforderliche Software so aufspielt, dass ausschließlich Daten des laufenden Telekommunikationsvorgangs erfasst werden. Die Ergebnisse werde ich im nächsten Tätigkeitsbericht erörtern.

### 7.5 Bundesamt für Verfassungsschutz

Schwerpunkte meiner Tätigkeit im Berichtszeitraum waren der Ausbau nachrichtendienstlicher Informationssysteme (vgl. u. Nr. 7.5.1) sowie die Umsetzung des Auskunftsverfahrens gem. § 15 Bundesverfassungsschutzgesetz im BfV (vgl. u. Nr. 7.5.2).

#### 7.5.1 Dürfen die Verfassungsschutzbehörden von Bund und Ländern einen umfassenden Informationspool einrichten?

*Der Ausbau nachrichtendienstlicher Informationssysteme der Verfassungsschutzbehörden des Bundes und der Länder zu umfassenden Wissensnetzen verstößt gegen gesetzliche Beschränkungen und ist daher nicht zulässig.*

Die Verfassungsschutzbehörden des Bundes und der Länder sind verpflichtet, in einer Hinweisdatei Identifikationsangaben, d. h. sog. Grunddaten, wie z. B. Name, Anschrift etc., sowie die Aktenzeichen zu denjenigen Personen und Organisationen zu speichern, die sie gemäß ihrem gesetzlichen Auftrag beobachten. Auf diese Weise weiß jede Verfassungsschutzbehörde, ob Informationen bei den anderen vorhanden sind. In dieser Datei ist aber nicht erkennbar, um welche Informationen es sich handelt und welchen Inhalt diese haben. Nur in gesetzlich eng gefassten Ausnahmefällen dürfen auch Textauszüge bzw. Textdateien in dieser Datenbank gespeichert werden.

Jetzt soll dieses Datensystem zu einem umfassenden Wissensnetz ausgebaut werden. Dies bedeutet einen Paradig-

menwechsel zu einem Informationspool, in den jeder Verbundpartner möglichst viele Daten zu relevanten Personen und Organisationen speichert. Diese Informationen könnten von den anderen Verbundteilnehmern unmittelbar eingesehen und automatisiert, z. B. durch eine Volltextrecherche, ausgewertet werden. Erste Realisierungsschritte haben bereits begonnen. Die bundesweite Inbetriebnahme eines derartigen Dateisystems soll im vierten Quartal 2011 erfolgen. Wesentliches Ziel ist u. a. die Speicherung von unstrukturierten Ursprungsdokumenten bzw. Ursprungsinformationen. Dies sind durch nachrichtendienstliche Mittel, d. h. durch heimliche Maßnahmen erhobene Daten sowie Informationen aus offenen Quellen (z. B. Zeitungsmeldungen oder Publikationen im Internet).

Problematisch ist, dass Ursprungsdokumente auch Daten von Personen enthalten (können), die nicht dem Aufgabenbereich des BfV unterfallen und die – jedenfalls bislang – nicht dateimäßig erfasst werden dürfen. Dies sind beispielsweise Daten von Minderjährigen unter 16 Jahren sowie von unbescholtenen Bürgerinnen und Bürgern, die als Randpersonen zufällig bzw. unbewusst mit einer Zielperson in Kontakt treten, z. B. Familienangehörige, Nachbarn, Kollegen, Vorgesetzte, Mitarbeiter oder auch Journalisten, die (beruflich) derartige Personen oder Organisationen kontaktieren bzw. über diese berichten. Deren Daten darf das BfV nach geltendem Recht allenfalls in Papierakten, nicht jedoch in Dateien speichern und keinesfalls für seine Tätigkeit auswerten. Mit Schaffung eines derartigen Wissensnetzes würde diese gesetzliche Speicherbeschränkung durchbrochen (wie bei DOMUS – vgl. 18. TB Nr. 14.1 und 20. TB Nr. 5.5.2).

Der Gesetzgeber hat die Unterscheidung zwischen einer Speicherung in Papierakten und in Dateien bewusst getroffen. Er wollte vermeiden, dass als Folge der Speicherung in einer Datei diese Daten – im Gegensatz zur Papierakte – technisch automatisiert in Sekundenbruchteilen aus einer immensen Fülle von Informationen herausgefiltert, ausgewertet und weltweit übermittelt werden können. Auch das Bundesverfassungsgericht hat stets betont, bereits durch die bloße Änderung einer Speicherung personenbezogener Daten von Papierakten in Dateien erfolge ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Denn in Dateien gespeicherte Daten sind – so das Bundesverfassungsgericht – im Gegensatz zur Speicherung in Akten technisch jederzeit und ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar. Dabei liegt nach Auffassung des Gerichts ein besonderes Eingriffspotential in der Menge der verarbeitbaren Daten, die auf konventionellem Wege gar nicht bewältigt werden könnte.

Das BMI meint, die Speicherung derartiger Personendaten in solchen Dateisystemen sei kein gesetzeswidriger Eingriff, da die Daten aufgrund technischer Sicherungen nicht eigenständig auswertbar sein sollen. Dies steht aber in Widerspruch zu den o. g. Vorgaben des Gesetzgebers und des Bundesverfassungsgerichts. Zudem können technische Sicherungen relativ schnell und einfach aufgehoben werden. Hierauf hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder anlässlich der 80. Sitzung am 3./4. November 2010 in einer Entschließung hingewiesen (vgl. Kasten zu Nr. 7.5.1).

Die Speicherung von Ursprungsdokumenten und -informationen in Wissensnetzen hätte auch schwerwiegende Konsequenzen: Sollte eine hiervon betroffene Person aufgrund ihrer zukünftigen Verhaltensweise, d. h. zu einem späteren Zeitpunkt, rechtlich zulässig in einer derartigen Datei gespeichert werden dürfen, könnte zu ihr eine umfassende, retrograde Suche und Auswertung in Bezug auf alle über sie vorhandenen Daten durchgeführt werden. Einbeziehbar wären auch diejenigen Daten, die gesetzeswidrig über diese Person gespeichert worden sind.

Fazit: Derartig ausgestaltete Dateisysteme entsprechen nicht dem geltenden Recht. Daher sind die bereits getroffenen Umsetzungsmaßnahmen umgehend auszusetzen. Das BMI hat mitgeteilt, dass es insoweit meiner Kritik Rechnung tragen wird, als Ursprungsdokumente, in denen unbeteiligte Dritte genannt sind, nicht gespeichert werden sollen.

Kasten zu Nr. 7.5.1

**Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. November 2010**

**Keine Volltextsuche in Dateien der Sicherheitsbehörden**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung und die Landesregierungen auf, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten.

Die Sicherheitsbehörden des Bundes und der Länder (Verfassungsschutz, Polizei) bauen zurzeit ihre elektronischen Dateisysteme aus. Dabei beziehen sie auch Daten mit ein, die bisher nur in Akten vorhanden sind, und streben eine umfassende Volltextverarbeitung mit Suchmöglichkeiten an. Nach jedem in einem Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird.

Dies hat gravierende Folgen: In Akten befinden sich auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten. Auch wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte und beiläufig in den Akten genannt wird, wird nun gezielt elektronisch recherchierbar.

Ein solcher Paradigmenwechsel steht im Widerspruch zum geltenden Recht. Danach dürfen die Sicherheitsbehörden nur unter restriktiven Voraussetzungen ausgewählte personenbezogene Daten in automatisierten Dateien speichern und übermitteln. Heute sind die zu speichernden Datenarten und Datenfelder in spezifischen Datei- und Errichtungsanordnungen genau festzulegen. Die Datenschutzbeauftragten müssen zuvor beteiligt werden.

Durch eine Volltextrecherche würden diese datenschutzrechtlichen Sicherungen aufgehoben. Die Zweckbindung der Datenverarbeitung wäre nicht mehr zu gewährleisten. Die gesetzlichen Begrenzungen sind von verfassungsrechtlichem Gewicht. Der Gesetzgeber hat bewusst engere Voraussetzungen vorgegeben, wenn personenbezogene Daten in IT-Systemen gespeichert werden. Denn elektronisch erfasste Daten können, wie das Bundesverfassungsgericht in ständiger Rechtsprechung betont, in Sekundenschnelle umfassend ausgewertet und ohne Rücksicht auf Entfernungen abgerufen werden. Damit würde in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung besonders intensiv eingegriffen, insbesondere wenn die Daten ohne Wissen der Betroffenen erhoben und verarbeitet werden.

Diese verfassungsrechtlich gebotenen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, insbesondere die informationelle Gewaltenteilung, würden hinfällig, wenn die unbegrenzte elektronische Volltexterfassung sämtlicher Informationen zugelassen würde.

Daran würde sich rechtlich nichts ändern, wenn technische Mechanismen derartige Auswertungen (vorübergehend) erschweren. Denn zum einen sind diese jederzeit technisch änderbar. Zum anderen würde eine vorübergehende Erschwerung der Recherchemöglichkeit weder den Eingriff in das Recht auf informationelle Selbstbestimmung noch den Verstoß gegen die vom Bundesverfassungsgericht vorgegebenen Grenzen einer Vorratsdatenverarbeitung beseitigen.

Bestehen diese Datenschutzrisiken schon bei allgemeinen Verwaltungsbehörden, sind sie bei den Sicherheitsbehörden umso gravierender. Dies gilt besonders für den Bereich der Nachrichtendienste, die auch Informationen zu legalem Verhalten und Erkenntnisse mit noch unklarer Relevanz sammeln dürfen. Für die – ggf. gänzlich unverdächtigen – Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Diese Risiken sind bei der Weiterentwicklung der IT-Systeme bereits in der Konzeptplanung zu berücksichtigen und auszuschließen.

### 7.5.2 Probleme beim Auskunftsrecht gegenüber dem Verfassungsschutz

*Werden Auskunftsverweigerungsgründe durch das BfV geltend gemacht, sind die hierfür tragenden Erwägungen zu dokumentieren. Dabei ist das BfV auch für Informationen verantwortlich, die es von den Landesämtern für Verfassungsschutz (LfV) erhalten hat.*

Das in § 15 BVerfSchG geregelte Auskunftsrecht ist von herausragender Bedeutung für die Wahrung des Grundrechts auf informationelle Selbstbestimmung. Bereits in meinem 22. TB (Nr. 4.7.1) hatte ich das BfV aufgefordert, seine Auskunftspraxis verfassungskonform auszugestalten. Nun gibt es erneut Anlass zu Kritik.

Nach § 15 Absatz 1 BVerfSchG erteilt das BfV einem Betroffenen über die zu seiner Person gespeicherten Daten Auskunft, soweit dieser hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an einer Auskunft darlegt. Hieran hat das BfV teilweise zu hohe Anforderungen gestellt.

Zudem hat es in gesetzlich festgelegten Fällen, in denen es eine Auskunft verweigern darf, keine angemessene und in den Akten nachvollziehbar dokumentierte Einzelfallabwägung vorgenommen, sondern die Auskunft pauschal verweigert.

Nach der Rechtsprechung des Bundesverfassungsgerichts ist dies nicht zulässig. In seiner Entscheidung vom 10. Oktober 2000 (1 BvR 586/90) hatte das Gericht ausgeführt, die Gründe der Auskunftsverweigerung seien aktenkundig zu machen, damit sie auch der Überprüfung durch Dritte zugänglich seien. Zudem müssten die der Auskunftsverweigerung zugrundeliegenden Abwägungen erkennbar und nachvollziehbar sein. Nach Gesprächen mit dem BfV konnte erreicht werden, dass diese verfassungsgerichtlichen Vorgaben nun in allen Fachabteilungen des Amtes umgesetzt werden. Damit kann ich zumindest unter Plausibilitätsgesichtspunkten die geltend gemachten Auskunftsverweigerungsgründe überprüfen, das Problem ist damit aber nur zum Teil gelöst:

Problematisch bleiben aber folgende Fälle: Verfügt das BfV zu einem Betroffenen über quellengeschützte Informationen, die es von einer anderen Stelle erhalten hat, kann es in aller Regel keine derartige Abwägung vornehmen, da ihm die hierfür notwendigen Hintergrundinformationen von diesen Stellen vielfach vorenthalten werden. Pauschale Mitteilungen dieser Stellen, wonach aus Quellenschutzgründen keine Auskunftserteilung erfolgen dürfe, berechtigen das BfV nicht zur Verweigerung der Auskünfte. Es ist weder datenschutz- noch verfassungsrechtlich hinnehmbar, dass die Betroffenen in diesen Fällen in gerichtlichen Verfahren ihr Auskunftsrecht durchsetzen müssen.

Ich plädiere an alle verantwortlichen Stellen, eine rechtskonforme Auskunftserteilung durch das BfV dringend zu gewährleisten

## 7.6 Nachrichtendienste

### 7.6.1 Datenverarbeitung beim BND

*Beim BND habe ich bei einer zentralen Großdatei mit mehreren Millionen Datensätzen datenschutzrechtliche Verstöße festgestellt. Bis zur Schaffung eines datenschutzrechtlich gesetzeskonformen Systems sollen die Daten nur noch in Ausnahmefällen operativ genutzt werden.*

Die festgestellten Verstöße beruhen im Wesentlichen auf strukturellen Defiziten dieser Großdatei. U. a. hat der BND keine den Vorgaben des § 5 Absatz 1 Bundesnachrichtendienstgesetz i. V. m. § 12 Bundesverfassungsschutzgesetz entsprechenden Wiedervorlage- und Löschungsüberprüfungen durchgeführt, so dass sich in dieser Datei eine Vielzahl von – offen und heimlich, d. h. mit nachrichtendienstlichen Mitteln erhobenen – Daten befindet, die längst auf ihre Erforderlichkeit hätten überprüft und ggf. gelöscht werden müssen. Ferner sind in diese seit vielen

Jahren bestehende Datei Altdaten, d. h. Daten, die sich schon vor der Errichtung dieser Datei im BND befanden, ungeprüft überführt worden. Deren Erfassungsdatum kann bis zur Gründung des BND zurückreichen.

Angesichts des immensen täglichen Datenzuflusses handelt es sich bei dieser Datei gleichsam um ein stetig anwachsendes informationelles Sammelbecken ohne Abfluss.

Nach intensiven Erörterungen der Problematik habe ich den BND und das Bundeskanzleramt als die zuständige Fachaufsichtsbehörde aufgefordert, eine gesetzeskonforme Handhabung dieser Datei zu gewährleisten. Nach Auffassung des BND handelt es sich bei der Datei um das „Rückgrat" des Dienstes, d. h. um einen unverzichtbaren Datenbestand, der aufgrund der enormen Datenmenge sowie der hiermit verbundenen technischen Schwierigkeiten gesetzeskonform in Gänze nicht mehr ausdifferenziert und den gesetzlichen Vorgaben gemäß bearbeitet werden kann. Hierzu sieht man sich erst nach dem Umzug des BND nach Berlin in der Lage. Um meinen Bedenken kurzfristig Rechnung tragen zu können, hat das Bundeskanzleramt vorgeschlagen, alle Daten, die länger als zehn Jahre gespeichert sind, aus dem aktuellen Online-Datenbestand in einen gesonderten Archivbestand zu überführen und diese nur in besonderen Fällen für aktuelle operative Zwecke weiter zu nutzen, z. B. für die Abwehr des Terrorismus oder die Bekämpfung von Proliferation.

Ich habe mich diesen Überlegungen nicht verschlossen, zumal der Archivbestand nach Aussage des Bundeskanzleramtes nur vorübergehend bis zur endgültigen gesetzeskonformen Ausgestaltung der Datei geführt werden soll. Über die weiteren Planungen soll ich rechtzeitig informiert werden.

### 7.6.2 Datenschutzrechtliche Verbesserungen bei der IT des MAD

*Differenzierte Zugriffsrechte, strukturierte Daten und Vermeidung von Paralleldatenbeständen: in einer neuen Datenbank beim Militärischen Abschirmdienst habe ich erfreuliche Ansätze für eine datenschutzkonformere Speicherung personenbezogener Daten durch Sicherheitsbehörden gefunden.*

Der MAD sah die Notwendigkeit, für die Abteilung III mit den Aufgabenbereichen „Spionageabwehr" und „Einsatzabschirmung" eine zentrale Datenbasis zu schaffen. Die Tendenz zur Zusammenführung bislang separat geführter Dateien in immer komplexeren Datenbanken sehe ich grundsätzlich kritisch, da die Bündelung von immer mehr personenbezogenen Daten aus unterschiedlichen Phänomenbereichen zwangsläufig mit einer höheren Eingriffsintensität in die Datenschutzrechte der Betroffenen einhergeht. Im vorliegenden Fall konnte ich meine diesbezüglichen Bedenken zurückstellen, wobei insbesondere die folgenden Punkte ausschlaggebend waren:

– Die personenbezogenen Daten aus den Bereichen „Einsatzabschirmung" und „Spionageabwehr" werden zwar in der neuen Datenbank zentral und damit redundanzfrei gespeichert, der automatisierte Zugriff bleibt jedoch durch dezidierte Zuweisung von differenzierten Rechten für die Nutzer auf die Datensätze des jeweiligen Aufgabenbereichs beschränkt. Gibt es im Rahmen einer Anfrage Treffer außerhalb der Zugriffsberechtigung, werden dem Nutzer nur Datensatztyp sowie Datensatznummer zusammen mit der speichernden Stelle ausgewiesen. Der Datensatz wird ggf. auf Antrag für den Sachbearbeiter frei geschaltet.

– In der Datenbank werden personenbezogene Informationen überwiegend strukturiert gespeichert. Die Befüllung erfolgt in Formularen über Auswahlfelder oder in relativ wenigen Freitextfeldern mit begrenzter Feldlänge. Zwar können Verweise zu Dateien beliebigen Formats in die Datensätze eingefügt werden, die so verknüpften Dateien sind jedoch über die Datenbank nicht suchfähig. Mit dieser Struktur wird ein Trend bei den Sicherheitsbehörden zur volltextmäßigen und prinzipiell umfassend recherchierbaren Speicherung unstrukturierter Ursprungsinformationen (vgl. o. Nr. 7.5.1) durchbrochen.

– Zur Darstellung fachlich relevanter Zusammenhänge verfügt die Datenbank über eine Schnittstelle zu einem Softwareprodukt, mit dessen Hilfe Informationen grafisch aufbereitet und analysiert werden. Ein direkter Zugriff auf den in Bearbeitung befindlichen Datenbestand – und damit auf personenbezogene Daten – ist dabei nicht möglich. Vielmehr werden die zur Visualisierung benötigten Daten innerhalb der Datenbank in einen eigenen Bereich kopiert. Dieser Bereich wird programmgesteuert täglich aktualisiert überschrieben. Eine Löschung oder Änderung im betroffenen Datensatz wird so automatisch auch in gespeicherte Grafiken und Analysen übernommen. Der Aufbau eines Paralleldatenbestandes ist damit ausgeschlossen.

– Die Protokollierung der Nutzeraktivitäten erfasst alle Datenbanktransaktionen. Ein geeignetes Tool zur Auswertung der Protokolldateien mit dem auch ad hoc Auswertungen im Rahmen einer datenschutzrechtlichen Kontrolle möglich sein sollen, wird bereitgestellt.

Nachdem die Datei in den Wirkbetrieb gegangen ist, beabsichtige ich, die Realisierung der beschriebenen Datenbankparameter einer datenschutzrechtlichen Kontrolle zu unterziehen.

## 7.7 Vorbeugender personeller Sabotageschutz – ein junges Verfahren, die alten Probleme

*Bei Kontrollen im vorbeugenden personellen Sabotageschutz festgestellte datenschutzrechtliche Mängel sind symptomatisch für das Sicherheitsüberprüfungsverfahren.*

Im Berichtszeitraum habe ich schwerpunktmäßig in zwei Unternehmen Sicherheitsüberprüfungen kontrolliert, die im Rahmen des 2002 eingeführten vorbeugenden perso-

nellen Sabotageschutzes (vgl. 19. TB Nr. 20.1) durchgeführt wurden.

Wie ich dabei feststellen musste, treten datenschutzrechtliche Mängel, die ich in der Vergangenheit schon mehrfach angesprochen hatte (vgl. 21. TB Nr. 5.8.3.2 und 22. TB Nr. 4.8.2), bedauerlicher Weise weiterhin auf.

Positiv bewerte ich es, dass die kontrollierten Unternehmen die Vorgaben des Sicherheitsüberprüfungsgesetzes (SÜG) für die Aufbewahrung der Sicherheitsakten einhalten. Gleichwohl gibt die Arbeitsplatzsituation des Sabotageschutzbeauftragten – insbesondere in kleineren Unternehmen – Anlass zur Kritik. So teilte sich dieser in einem Fall sein Büro und einen Netzwerkdrucker mit anderen Unternehmensangehörigen, die nicht mit Aufgaben der Sicherheitsüberprüfung betraut waren. Ich habe in diesem Zusammenhang das für diese Sicherheitsüberprüfungen zuständige BMWi erneut darauf hingewiesen, dass die Einrichtung eines Einzelbüros für die ausschließliche Benutzung durch den Sabotageschutzbeauftragten geboten ist. Ein mit Stellwänden in einem Großraumbüro abgetrennter Bereich gewährleistet meines Erachtens nicht, dass die Kenntnisnahme von sensiblen, im Rahmen der Sicherheitsüberprüfung erhobenen und verarbeiteten personenbezogenen Daten durch unbefugte Dritte ausgeschlossen wird.

Immer noch aktuell ist der Umfang des Zugriffs des Sabotageschutzbeauftragten auf das Personalverwaltungssystem des jeweiligen Unternehmens: In einem Unternehmen übermittelte die Personalabteilung in regelmäßigen Abständen die Daten aller Mitarbeiter an den Sabotageschutzbeauftragten, wodurch dieser auch die Daten von Personen erhielt, die nicht seiner Zuständigkeit unterfielen. Meine früher geäußerte Befürchtung (vgl. 22. TB Nr. 4.8.2), dass diese Praxis nicht auf Einzelfälle beschränkt sei, hat sich damit bestätigt. Ich wiederhole daher meine Forderung nach einer Regelung, die klarstellt, ob und in welchem Umfang dem Sabotageschutzbeauftragten bzw. dem Sicherheitsbevollmächtigten der Zugriff auf Personaldaten zu gestatten ist.

In beiden überprüften Unternehmen ergaben sich datenschutzrechtliche Probleme aufgrund der dort geübten Praxis, Mitarbeiterinnen und Mitarbeiter, für die eine Sicherheitsüberprüfung im Rahmen des vorbeugenden personellen Sabotageschutzes beantragt wurde, vor Abschluss der Sicherheitsüberprüfung und ohne eine formelle vorläufige Zuweisung mit der sicherheitsempfindlichen Tätigkeit zu betrauen: Wird nämlich die Sicherheitsüberprüfung mit dem Ergebnis abgeschlossen, dass keine Ermächtigung zu einer sicherheitsempfindlichen Tätigkeit erteilt werden kann, ergibt sich die Frage, wie lange die Sicherheitsakte aufzubewahren ist. Wurde noch keine sicherheitsempfindliche Tätigkeit aufgenommen, sind die Unterlagen nach einem Jahr zu vernichten. Nach vorherigem Einsatz an einer sicherheitsempfindlichen Stelle müssen sie hingegen fünf Jahre aufbewahrt werden. Die Sicherheitsüberprüfung im Rahmen des vorbeugenden personellen Sabotageschutzes ist ein formalisiertes Verfahren, das eine Beschäftigung mit einer sicherheitsempfindlichen Tätigkeit ohne eine bereits abgeschlossene oder vorläufige Überprüfungsmaßnahme im Sinne des SÜG nicht zulässt. Ein Unternehmen, das Beschäftigte ungeachtet dessen an einer sicherheitsempfindlichen Stelle einsetzt, entspricht damit nicht den gesetzlichen Vorgaben. Diese faktische, rechtlich unzulässige Tätigkeitsaufnahme würde den Betroffenen zum Nachteil gereichen, wenn an dieses rechtswidrige faktische Vorgehen die Rechtsfolge einer fünfjährigen Speicherung anknüpfen würde. Ich habe daher gefordert, die Unterlagen in diesen Fällen nach einem Jahr zu vernichten.

Aus den von mir geprüften Sicherheitsakten ergab sich weiterhin, dass Kopien von Reisepässen der Betroffenen zu den Unterlagen genommen worden waren. Dies entspricht ebenfalls nicht den gesetzlichen Vorgaben. Im Rahmen des Sabotageschutzes ist eine einfache Sicherheitsüberprüfung durchzuführen. Die personenbezogenen Daten, die in diesem Zusammenhang erhoben werden dürfen, sind im SÜG abschließend aufgezählt. Die Ablichtung eines Ausweisdokumentes darf in diesen Fällen nicht zur Sicherheitsakte genommen werden. Der Sabotageschutzbeauftragte wies mich in diesem Zusammenhang auf ein Schreiben des BMWi hin, wonach das Bundesamt für Verfassungsschutz als mitwirkende Behörde die Vorlage einer Passkopie zur Überprüfung bestimmter Antragsteller benötige. Ich habe das BMWi hierzu um Stellungnahme gebeten, die bei Redaktionsschluss noch nicht vorlag.

# 8 Innere Verwaltung und Rechtswesen

## 8.1 Statistik

### 8.1.1 Zensus 2011

*Der Startschuss für den Zensus 2011 ist gefallen. Zum ersten Mal seit 1987 (in den alten Bundesländern) bzw. 1981 (in den neuen Bundesländern) findet in Umsetzung der Verordnung (EG) Nr. 763/2008 auch in Deutschland wieder eine Volkszählung statt, wenn auch im wesentlichen als Registerzählung.*

Zum Stichtag 1. November 2010 haben sämtliche Meldebehörden des Landes ihre Datensätze an die Statistischen Ämter übermittelt. Weitere Datenlieferungen folgen zum 9. Mai sowie zum 9. August 2011. Ebenfalls zum 9. Mai 2011 finden eine Gebäude- und Wohnungszählung, eine Haushaltestichprobe sowie Erhebungen in Sonderbereichen statt.

Rechtsgrundlage für die Volkszählung ist das Gesetz über den registergestützten Zensus im Jahre 2011 (Zensusgesetz 2011 – ZensG 2011), das am 16. Juli 2009 in Kraft getreten ist. Zu den Inhalten des mir damals vorliegenden Entwurfs habe ich bereits berichtet (vgl. 22. TB Nr. 5.5). Bedauerlicherweise ist man meiner Forderung, auf personenbezogene Erhebungen in den sensiblen Sonderbereichen (d. h. Gemeinschaftsunterkünfte, bei denen allein die Information über die Zugehörigkeit für die Betroffenen die Gefahr einer sozialen Benachteiligung hervorrufen könnte, z. B. Justizvollzugsanstalten) gänzlich zu verzichten, nicht nachgekommen.

Darüber hinaus ist im Laufe des Gesetzgebungsverfahrens der Merkmalskatalog bei der Haushaltebefragung erweitert worden. Die Erhebungsmerkmale „rechtliche Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft“ sowie „Bekenntnis zu einer Religion, Glaubensrichtung oder Weltanschauung“ sind europarechtlich nicht vorgegeben. Im Gesetzgebungsverfahren habe ich die Erforderlichkeit und Eignung dieser Erhebungsmerkmale wiederholt in Frage gestellt. Leider ist man mir in diesem Punkt nicht gefolgt und hat die Merkmale in das ZensG 2011 aufgenommen. Immerhin konnte aber erreicht werden, dass die Beantwortung der Frage nach dem Glaubensbekenntnis freiwillig ist.

Bei der Gebäude- und Wohnungszählung werden sämtliche Eigentümerinnen und Eigentümer von Gebäuden und Wohnungen zu diesen schriftlich befragt. Gefragt wird beispielsweise nach dem Baujahr des Gebäudes, der Heizungsart, der Art der Nutzung und der Fläche der Wohnung (§ 6 Absatz 2 ZensG 2011).

Im Rahmen der Haushaltestichprobe werden 9,6 Prozent der Bevölkerung aufgefordert, Angaben zu machen. Die Fragen umfassen persönliche Angaben, Angaben über Bildung und Ausbildung sowie Angaben den Beruf betreffend (§ 7 Absatz 4 ZensG 2011). Bei den Erhebungen in den Sonderbereichen werden für jede dort wohnende Person beispielsweise Monat und Jahr der Geburt, der Familienstand und der Tag des Bezugs der Wohnung bzw. des Beginns der Unterbringung erfragt (§ 8 Absatz 1 Nr. 1 ZensG 2011). Wenngleich der Gesetzgeber entgegen meiner Forderung leider nicht auf personenbezogene Erhebungen in den sensiblen Sonderbereichen verzichten wollte, hat das Statistische Bundesamt zumindest für die Verarbeitung dieser Daten ein spezielles Verfahren entwickelt, das den besonderen Schutzbedarf der an diesen Anschriften lebenden Personen berücksichtigt.

Besonders schützenswert sind auch diejenigen Personen, für die im Melderegister eine Übermittlungssperre wegen Gefahr für Leib oder Leben eingetragen ist. Hierbei handelt es sich beispielsweise um Personen im Zeugenschutzprogramm. Um dem besonderen Schutzbedarf dieser Personen Rechnung zu tragen, habe ich empfohlen, diejenigen Anschriften, an denen eine Person mit einem solchen Sperrvermerk lebt, insgesamt aus der Haushaltestichprobe auszunehmen.

Für die Durchführung des Zensus 2011 haben die Statistischen Ämter ein generisches Sicherheitskonzept erstellt, welches mir zur Prüfung vorgelegen hat. Das Konzept orientiert sich methodisch an den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgegeben Standards. § 13 ZensG 2011 sieht vor, dass u. a. für jede Person eine Ordnungsnummer vergeben wird. Mir war es besonders wichtig, dass es nicht möglich ist, von der Ordnungsnummer auf die dahinter stehende Person schließen zu können. Ich habe daher mit dem Statistischen Bundesamt vereinbart, dass die personenbezogene Ordnungsnummer mit Hilfe einer sogenannten Hashfunktion verschlüsselt wird.

Neben den Ordnungsnummern im Sinne des § 13 ZensG 2011 werden statistikintern weitere Nummern vergeben, die nur der Organisation des jeweiligen konkreten Erhebungsgeschäftes dienen. Eine solche Nr. ist die Auskunftspflichtigen-ID im Rahmen der Gebäude- und Wohnungszählung. Sie dient dazu, statistikintern eine bestimmte Person zu identifizieren und deren Daten im Rahmen der Gebäude- und Wohnungszählung zusammenzuführen. Zwar besteht die Auskunftspflichtigen-ID aus einer fortlaufend gebildeten Ziffernfolge, aus der keine Informationen ableitbar sind. Als statistikinterner Identifikator darf sie dennoch den abgeschotteten Bereich der Statistik nicht verlassen. Hiervon konnte ich auch das Statistische Bundesamt überzeugen. Entgegen der ursprünglichen Planung wurde auf die Nutzung der Auskunftspflichtigen-ID als Fragebogennummer für die Fragebögen der Gebäude- und Wohnungszählung verzichtet und stattdessen wird für jeden Fragebogen eine nicht systematische Fragebogennummer vergeben, die innerhalb der amtlichen Statistik mit Hilfe einer algorithmischen Umrechnung mit der Auskunftspflichtigen-ID in Beziehung gesetzt wird.

Die praktische Durchführung des Zensus 2011 werde ich intensiv und in enger Kooperation mit den für die Statistischen Landesämter, die Städte und Gemeinden zuständigen Landesdatenschutzbeauftragten kritisch begleiten und dabei insbesondere auf

– die Einhaltung der gesetzlichen Zweckbindung,

– die frühestmögliche Datenlöschung und

– eine hohe Datensicherheit

achten.

### 8.1.2 Statistikdaten dürfen nicht beschlagnahmt werden

*Ein Beschluss des Landgerichts Mannheim stellt klar, dass Einzelangaben über persönliche und sachliche Verhältnisse, die für eine Bundesstatistik mit Auskunftspflicht erteilt werden, ohne Zustimmung des Betroffenen in strafrechtlichen Ermittlungsverfahren nicht gegen ihn verwertet werden dürfen.*

Gegen den Beschuldigten lief ein Ermittlungsverfahren wegen des Verdachts der Steuerhinterziehung. Da die betroffenen Unternehmen im Rahmen der statistischen Erhebung für die Außenhandelsstatistik Umsatzdaten an das Statistische Bundesamt gemeldet hatten, wurden auf der Grundlage eines Durchsuchungs- und Beschlagnahmebeschlusses Unterlagen beim Statistischen Bundesamt beschlagnahmt.

In seinem Beschluss vom 18. Juli 2007 (22 Qs 7/06) stellt das LG Mannheim fest, dass diese Durchsuchungs- und Beschlagnahmeanordnung rechtswidrig war. Die vom Statistischen Bundesamt erhobenen Angaben zur Außenhandelsstatistik unterlägen im Strafverfahren gegen die Verantwortlichen der betroffenen Unternehmen einem Verwertungsverbot. Das in § 16 Bundesstatistikgesetz vorgegebene Statistikgeheimnis sei verfassungskonform

dahin auszulegen, dass Einzelangaben über persönliche und sachliche Verhältnisse, die für eine Bundesstatistik gemacht würden, ohne Zustimmung des Betroffenen im strafrechtlichen Ermittlungsverfahren nicht gegen ihn verwertet werden dürften. Eine gegen den Willen des Betroffenen erfolgende Verwertung dieser Angaben sei nicht mit dem grundrechtlich geschützten Grundsatz vereinbar, dass niemand sich selbst belasten müsse.

Im Rahmen der Außenhandelsstatistik bestünden mit Beugemitteln erzwingbare Auskunftspflichten. Die betroffenen Unternehmen seien uneingeschränkt verpflichtet, gegenüber dem Statistischen Bundesamt wahrheitsgemäße Angaben zu machen, insbesondere sei kein Auskunftsverweigerungsrecht für den Fall einer drohenden Selbstbezichtigung vorgesehen. Das strafprozessuale Verweigerungsrecht liefe aber ins Leere, wenn eine außerhalb des Strafverfahrens erzwungene Selbstbezichtigung gegen den Willen des Auskunftspflichtigen strafrechtlich zu dessen Nachteil verwendet werden dürfe.

Eine erfreuliche Entscheidung!

## 8.2 Ausländerrecht

### 8.2.1 Ausländerzentralregister – Daten von Unionsbürgern endlich besser schützen!

*Die europarechtlichen Vorgaben, wann Daten zu Unionsbürgern gespeichert werden dürfen, setzt das Ausländerzentralregister (AZR) nur unzureichend um. Jetzt ist der Gesetzgeber am Zug.*

Im Ausländerzentralregister (AZR) sind personenbezogene Daten von allen Ausländern erfasst, die sich länger als drei Monate in Deutschland aufhalten, darunter auch die Daten von Unionsbürgern. Der EuGH hatte mit Urteil vom 16. Dezember 2008 (C-524/06) diese Speicherung von Daten zu Unionsbürgern in einem zentralen Register wie dem AZR sowie deren Übermittlung an andere Behörden nur unter engen Voraussetzungen für zulässig gehalten (vgl. 22. TB Nr. 16.1). Diese Entscheidung habe ich zum Anlass für eine datenschutzrechtliche Kontrolle beim AZR genommen. Wie ich dabei feststellen musste, sind die Vorgaben des EuGH im automatisierten Abrufverfahren und damit für einen Großteil der Abrufe nicht umgesetzt worden. Auch waren bestehende Suchvermerke zu Unionsbürgern noch nicht gelöscht. Damit konnten weiterhin die im AZR gespeicherten Daten zu Unionsbürgern, z. B. zum Zwecke der Kriminalitätsbekämpfung, an Sicherheitsbehörden übermittelt werden, obwohl der EuGH dies ausdrücklich für unzulässig erklärt hatte. Diesen Verstoß gegen europarechtliche Vorgaben habe ich nach § 25 Absatz 1 Nr. 1 BDSG beanstandet. Durch die Registerbehörde waren auch keine technisch-organisatorischen Maßnahmen ergriffen worden, die einen Abruf der Daten nur zu den vom EuGH anerkannten ausländerrechtlichen Zwecken und nur durch die in diesem Bereich zuständigen Behörden ermöglicht hätten.

Das Bundesministerium des Innern (BMI) hat daraufhin zugesagt, noch bestehende Suchvermerke zu Unionsbürgern zu löschen. Die technische Umsetzung der Vorgaben für das automatisierte Abrufverfahren soll unmittelbar nach Abschluss eines derzeit eingeleiteten Gesetzgebungsverfahrens zur Änderung des AZR-Gesetzes erfolgen. Der im Rahmen der Ressortabstimmung vom BMI zunächst vorgelegte Referentenentwurf setzte die Vorgaben des EuGH allerdings nur unzureichend in nationales Recht um. Deswegen habe ich mich dafür eingesetzt, sowohl den Umfang der im AZR gespeicherten Daten zu Unionsbürgern deutlich zu reduzieren als auch die Übermittlung dieser Daten ausschließlich zu aufenthaltsrechtlichen Zwecken und nur an die in diesem Bereich zuständigen Behörden zuzulassen.

Das Gesetzgebungsverfahren war zum Redaktionsschluss noch nicht abgeschlossen. Ich werde es weiterhin begleiten und mich nach dessen Abschluss für eine zeitnahe technische Umsetzung im AZR einsetzen.

Die im Zusammenhang mit der Änderung des AZR-Gesetzes nun beabsichtigte Aufnahme der bereits im Jahr 2007 unter meiner Beteiligung zwischen den Ressorts abgestimmten Forschungsklausel ist hingegen positiv zu bewerten (vgl. 21. TB Nr. 7.1.3). Damit wird es künftig möglich sein, die im AZR enthaltenen Daten von Drittstaatsangehörigen für wissenschaftliche Zwecke zu nutzen.

### 8.2.2 Elektronischer Aufenthaltstitel – Dokument im Scheckkartenformat mit Fingerabdrücken

*Im Zuge der Einführung des elektronischen Aufenthaltstitels werden Ausländerbehörden künftig obligatorisch neben einem Lichtbild auch Fingerabdrücke von in Deutschland lebenden Ausländern erfassen.*

In Umsetzung einer europäischen Vorgabe (Verordnung (EG) 380/2008) hat das Bundesministerium des Innern die rechtliche Grundlage für die Einführung elektronischer Aufenthaltstitel für Ausländer, die keine Unionsbürger sind, erarbeitet. Voraussichtlich ab September 2011 soll die neue elektronische Aufenthaltskarte – wie der neue Personalausweis (nPA – vgl. Nr. 3.2) – im Scheckkartenformat ausgegeben werden. Die Aufenthaltskarte wird einen Chip enthalten, auf dem zwei Fingerabdrücke und ein digitales Lichtbild des Inhabers als biometrische Merkmale gespeichert sind, wozu die europäische Verordnung verpflichtet (vgl. Kasten zu Nr. 8.2.2). Anders als beim nPA ist die Aufnahme der Fingerabdrücke beim elektronischen Aufenthaltstitel obligatorisch.

Als Zusatzfunktion verfügt die neue Aufenthaltskarte zudem über die Möglichkeit des elektronischen Identitätsnachweises (eID), der die Inhaber bei Rechtsgeschäften im Internet legitimieren kann.

Im Rahmen meiner Beteiligung am Gesetzgebungsverfahren habe ich mich für ein hohes Datenschutz- und Datensicherheitsniveau bei den auf dem Chip gespeicherten biometrischen Merkmalen und der eID-Funktion eingesetzt. Dies soll durch eine entsprechende Anwendung der datenschutzrechtlichen Bestimmungen sicher gestellt werden,

die bereits für Reisepässe (hinsichtlich der biometrischen Merkmale vgl. 22. TB Nr. 6.3.1) und den neuen Personalausweis (hinsichtlich der eID-Funktion vgl. Nr. 3.2 und 22. TB Nr. 3.3) gelten. Ich werde aufmerksam verfolgen, ob diese datenschutzrechtlichen Anforderungen umgesetzt werden. Das gilt insbesondere für die Frage des Zugriffsschutzes hinsichtlich der im Chip gespeicherten biometrischen Daten.

Ebenso trete ich Forderungen entgegen, die biometrischen Merkmale zusätzlich in zentralen Registern wie etwa dem Ausländerzentralregister zu erfassen.

Kasten zu Nr. 8.2.2

Elektronischer Aufenthaltstitel für Ausländer


## 8.3 Nationales Waffenregister

*Bei den Planungen zum Nationalen Waffenregister (NWR) müssen angemessene datenschutzrechtliche Vorkehrungen getroffen werden.*

Nach Artikel 4 Absatz 4 der EG-Waffenrichtlinie (91/477/EWG) müssen die EU-Mitgliedstaaten spätestens bis Ende 2014 ein computergestütztes Waffenregister einführen. Das deutsche Waffengesetz sieht die Einführung des Registers bereits bis zum 31. Dezember 2012 vor. Die Innenministerkonferenz hat sich dafür ausgesprochen, dass Bund und Länder gemeinsam ein einheitlich organisiertes computergestütztes Nationales Waffenregister errichten. Die Federführung haben der Bund und das Land Baden-Württemberg übernommen.

Realisiert werden soll das zentrale Register beim Bundesverwaltungsamt (Registerbehörde). Die berechtigten Behörden sollen bedarfsgerecht auf die erforderlichen Daten des NWR zugreifen können: Für jede erlaubnispflichtige Waffe soll zeitnah nachvollziehbar sein, wer Besitzer der Waffe ist, seit wann er die Waffe besitzt und wo bzw. von wem sie erworben wurde. Der Weg einer erlaubnispflichtigen Waffe soll über den aktuellen Besitzer hinaus über etwaige Vorbesitzer bis hin zum Waffenhersteller oder -importeur zurückzuverfolgen sein. Das NWR soll die Voraussetzung dafür schaffen, die in derzeit ca. 570 Waffenbehörden – auf Basis unterschiedlicher Software oder in Einzelfällen noch per Kartei erfassten – Informationen aufzubereiten und in ein abgestimmtes computergestütztes System zu überführen. Dadurch soll zugleich ein Beitrag zur Verbesserung der öffentlichen Sicherheit geleistet werden.

Positiv sehe ich es, dass § 43a des Waffengesetzes durch ein eigenes Errichtungsgesetz und eine Rechtsverordnung ergänzt werden soll. Hierbei werde ich darauf achten, dass

- ein enger Merkmalskatalog sich an der Vorgabe der EG-Waffenrichtlinie orientiert,
- eine Doppelspeicherung von Daten auf Bundesebene und in den Ländern vermieden wird,
- angesichts der Grundentscheidung für ein zentrales Register die Speicherung der bundesweit relevanten Daten ausschließlich auf Bundesebene vorgesehen wird, wobei Datenspeicherung und Datenpflege verantwortlich durch die Waffenbehörden in den Ländern erfolgen sollten.

## 8.4 Register der Entscheidungen in Staatsangehörigkeitsangelegenheiten

*Das Register der Entscheidungen in Staatsangehörigkeitsangelegenheiten (EStA) muss datenschutzgerecht ausgestaltet werden.*

Nach § 33 Absatz 1 des Staatsangehörigkeitsgesetzes (StAG) führt das Bundesverwaltungsamt (BVA) das Register EStA. Zur Organisation, IT-Umsetzung und Führung dieses Registers habe ich das BMI und das BVA in einzelnen Fragen beraten, die durch das Gesetz nicht abgebildet werden.

Bei Staatsangehörigkeitsentscheidungen, die lediglich eine Feststellung der deutschen Staatsangehörigkeit zum Inhalt haben, hatte das BMI darum gebeten, dass trotz fehlender ausdrücklicher Rechtsgrundlage der dem Erwerb der Staatsangehörigkeit zugrundeliegende Rechtsgrund und das dazugehörige Datum in EStA ausnahmsweise gespeichert werden dürfen. Bis zum Inkrafttreten der auch insoweit beabsichtigten Gesetzesänderung halte ich eine datenschutzgerechte Ausnahmeregelung, die den administrativen Bedürfnissen gerecht wird, dann für vertretbar, wenn nachstehende Vorkehrungen getroffen werden, denen das BVA bereits nachkommt. Die Daten sind mit einer „qualifizierten“ Sperre zu versehen (§ 3 Absatz 4 Nr. 4 BDSG), d. h. die Übermittlung an betroffene Auskunftssu-

chende ist seitens der Registerbehörde (BVA) einer strengen Prüfung zu unterziehen und insbesondere davon abhängig zu machen, dass Auskunftssuchende ein konkretes Bedürfnis am Erhalt gerade dieser Informationen nachweisen oder glaubhaft machen und auch im Übrigen keine Gründe der Übermittlung entgegenstehen. Ferner muss die Verwendung dieser Daten dokumentiert werden.

Weitere Punkte betreffen vorläufige Modalitäten zur datenschutzgerechten Einrichtung von Freitextfeldern in IT-Eingabemasken, Arbeitshinweise an die betreffenden BVA-Mitarbeiter für den Umgang mit dem Register EStA, Löschungsfristen für gespeicherte staatsangehörigkeitsrechtliche Entscheidungen und für Daten der Zugriffsprotokollierung, Auslegung und Handhabung des § 33 Absatz 2 Nr. 1 StAG (Aufnahme von Ordens- oder Künstlername) sowie die Speicherung von Auflagen. Dabei dienten die für das Ausländerzentralregister bestehenden Regelungen als Vorbild.

Bei der Novellierung des Staatsangehörigkeitsgesetzes werde ich darauf achten, dass an die Stelle der Übergangsregelungen bald eine tragfähige gesetzliche Grundlage tritt.

## 8.5 Die Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR

### 8.5.1 Kontrollen in zwei Außenstellen

*Bei der Kontrolle der Bearbeitung von Anträgen auf Akteneinsicht oder Herausgabe von Duplikaten von Stasi-Unterlagen stand die Anonymisierung personenbezogener Angaben im Mittelpunkt. Geprüft wurde ferner die Verwendung der Unterlagen für die politische und historische Aufarbeitung im Rahmen von Forschungsanträgen. Datenschutzmängel habe ich nicht festgestellt.*

Bei der Kontrolle des datenschutzgerechten Arbeitsablaufs von Anträgen auf Akteneinsicht oder Herausgabe von Duplikaten von Stasi-Unterlagen gem. §§ 12 ff. Stasi-Unterlagen-Gesetz (StUG) habe ich schwerpunktmäßig die organisatorischen und verfahrensmäßigen Modalitäten der in diesem Zusammenhang notwendigen Anonymisierung personenbezogener Daten geprüft.

Die Anonymisierung dient dem Schutz Betroffener oder Dritter, deren personenbezogene Informationen dem Antragsteller nicht zugänglich zu machen sind. Die BStU hat mir einen Arbeitsplatz zur Anonymisierung von Stasi-Unterlagen vorgestellt und das Verfahren erläutert. Sie stellte dar, dass es sich bei den zu anonymisierenden Angaben nicht nur um personenbezogene Daten als solche, sondern auch um Informationen über Begleitumstände handeln könne, soweit daraus Rückschlüsse auf eine bestimmte Person gezogen werden könnten. Da es verschiedene Ansätze für eine fachlich korrekte Anonymisierung gibt, legt die BStU großen Wert auf Fragen zur Aus- und Fortbildung der damit betrauten Mitarbeiter. Dies betrifft u. a. die Frage einer einheitlichen Handhabung bestimmter Fallkonstellationen. Grundlage hierfür ist eine Anonymisierungsrichtlinie zu den entsprechenden Vorschriften im StUG. Ich habe festgestellt, dass die BStU diesem Komplex einen hohen Stellenwert beimisst und ein in sich stimmiges Bearbeitungs- und Fortbildungsverfahren eingeführt hat, was ich sehr begrüße.

Die Kontrolle bei einer anderen Außenstelle hatte Einzelaspekte der Nutzung der Stasi-Unterlagen für Zwecke der Forschung und der Medien gem. §§ 32 bis 34 StUG zum Inhalt, insbesondere auch Fragen der einheitlichen Bewertung und Entscheidung über Anträge zu Forschungsvorhaben.

Die Grundentscheidung, ob die Nutzung bestimmter Stasi-Unterlagen für Zwecke der Forschung und der Medien gem. §§ 32 bis 34 StUG erfolgen kann, wird in der BStU-Zentrale Berlin getroffen. Bei dieser Entscheidung werden Themenstellung, MfS-Bezug und Veröffentlichungsabsicht des Antragstellers als Kriterien berücksichtigt. Die Zentralisierung der Grundentscheidung halte ich für sinnvoll, da dadurch von vornherein die Einheitlichkeit der Beurteilung entsprechender Anträge gewährleistet werden kann.

Ferner habe ich geprüft, ob und wie die Antragsteller über die Sensibilität der erhaltenen Stasi-Unterlagen und insbesondere hinsichtlich der Veröffentlichung der gewonnenen Ergebnisse durch die Außenstelle informiert bzw. belehrt werden. Die BStU hat nicht nur – wie im 22. TB Nr. 5.8 dargestellt – zu den entsprechenden gesetzlichen Regelungen des StUG Auslegungsvorschriften und Anwendungshinweise erlassen, die sich primär an die Mitarbeiter richten, sondern hat auch Maßnahmen vorgesehen, die die Antragsteller betreffen. Die Forscher erhalten einen Gesetzesauszug zu den einschlägigen Bestimmungen der §§ 32 bis 34 StUG, der ihnen zudem ausführlich in einem Gespräch erläutert wird. Darüber hinaus haben sie den Erhalt von Duplikaten gem. § 33 StUG, deren zweckentsprechende Verwendung sowie die Kenntnisnahme des besonderen Hinweises, dass „personenbezogene Informationen nur unter Beachtung von § 32 Absatz 3 StUG veröffentlicht werden dürfen“, schriftlich zu bestätigen. Die so erfolgte Einbeziehung der Antragsteller als externe Personen in die Verantwortung über die sensiblen Stasi-Unterlagen entspricht dem Willen des Gesetzes.

Bei den Kontrollen wurden erfreulicher Weise keine Datenschutzmängel festgestellt.

### 8.5.2 Virtuelle Rekonstruktion zerrissener Stasi-Unterlagen

*Bei der Rekonstruktion zerrissener Stasi-Unterlagen müssen ebenso wie bei unversehrten Stasi-Unterlagen geeignete Datenschutzvorkehrungen getroffen werden.*

Eine manuelle Rekonstruktion zerrissener MfS-Unterlagen ist kaum geeignet, die sehr große Menge der vorhandenen Fragmente in einer angemessenen Zeit zu verarbeiten. Angesichts des insgesamt bedeutenden Inhalts der zu rekonstruierenden Unterlagen einerseits und des sehr hohen Zeitbedarfs für eine manuelle Rekonstruktion andererseits forderte im Jahr 2000 eine überwältigende Mehrheit der Abgeordneten des Deutschen Bundestags, geeignete Verfahren zu erproben, mit denen die Rekonstruktion vor-

vernichteter Stasi-Unterlagen auf elektronischem Wege beschleunigt werden kann (vgl. Bundestagsdrucksache 15/4885). Ein entsprechendes Pilotprojekt wurde in der 1. Jahreshälfte 2007 gestartet.

Zerrissene Stasi-Unterlagen sind von gleicher datenschutzrechtlicher Sensibilität wie regulär erhaltene, da sie personenbezogene Daten (auch entsprechende Begleitumstände) zum Inhalt haben. Sie bedürfen daher gleichwertiger Datenschutzvorkehrungen. Ihre IT-unterstützte virtuelle Rekonstruktion erfolgt derzeit unter Einbeziehung einer wissenschaftlichen externen Stelle. Dies erfordert zusätzlich entsprechende Vorkehrungen für eine datenschutzgerechte Auftragsdatenverarbeitung und hinsichtlich der IT-Sicherheit. Bei meinem Informationsbesuch habe ich die BStU zu projektrelevanten Fragen der Auftragsdatenverarbeitung beraten. Diese Beratung bezog sich insbesondere darauf, dass für bestimmte Fragen § 11 BDSG analog angewendet werden sollte, soweit § 41 Absatz 3 StUG keine hinreichend konkreten Regelungen zur Auftragsdatenverarbeitung enthält (vgl. zur Auftragsdatenverarbeitung auch Nr. 2.4 und 8.5.3).

Ich werde dieses Projekt weiterhin begleiten und die BStU in Datenschutzfragen beraten.

### 8.5.3 Geplante Änderung des Stasi-Unterlagen-Gesetzes

*Die Möglichkeit, bestimmte Personen auf eine frühere Stasi-Tätigkeit zu überprüfen, soll erneut verlängert und zugleich der überprüfbare Personenkreis im öffentlichen Dienst wieder erweitert werden. Bei dieser Gelegenheit sollten auch Regelungslücken im StUG zur Auftragsdatenverarbeitung geschlossen werden.*

Die im StUG vorgesehene Möglichkeit, Stasi-Unterlagen zur Überprüfung bestimmter Personen auf eine frühere Stasi-Tätigkeit zu verwenden, war ursprünglich bis Ende 2006 befristet. Wie im 21. TB (Nr. 7.2.1) berichtet, wurde diese Frist bereits einmal durch den Gesetzgeber bis Ende 2011 verlängert und gleichzeitig der überprüfbare Personenkreis im öffentlichen Dienst erheblich eingeschränkt (7. StUÄndG vom 21. Dezember 2006, BGBl. I S. 3326).

Der Beauftragte der Bundesregierung für Kultur und Medien hat nunmehr einen Gesetzentwurf in die Ressortabstimmung gegeben, der eine nochmalige Verlängerung der Überprüfungsfristen bis 2019 vorsieht. Außerdem sollen künftig wieder weitere Personengruppen des öffentlichen Dienstes auf eine Stasi-Vergangenheit überprüfbar sein. Ich habe im Rahmen meiner Beteiligung darauf gedrängt, dass nachvollziehbar dargelegt wird, aus welchen Gründen und für welche konkreten Fallgruppen sich die vom Gesetzgeber des 7. StUÄndG noch für richtig gehaltene Begrenzung des Personenkreises nicht bewährt hat. Außerdem habe ich mich dafür eingesetzt, dass der künftig überprüfbare Personenkreis hinreichend normenklar, etwa durch die Orientierung an bestimmten Besoldungsgruppen o. Ä., im Gesetz bezeichnet wird.

Des Weiteren habe ich angeregt, das Gesetzgebungsvorhaben auch dazu zu nutzen, die im Rahmen meiner Beratungstätigkeit festgestellte Rechtsunsicherheit bei Fragen der Auftragsdatenverarbeitung (vgl. o. Nr. 8.5.2) zu beseitigen und ausdrücklich im StUG zu regeln, dass auch dort die umfassenden verfahrensmäßigen Absicherungen des § 11 BDSG analoge Anwendung finden.

Das Gesetzgebungsverfahren war bei Redaktionsschluss noch nicht abgeschlossen. Ich werde es weiterhin aufmerksam begleiten.

## 8.6 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK); Bundesanstalt Technisches Hilfswerk (THW)

*Die Komplexität des Bevölkerungs-/Zivilschutzes in Deutschland erfordert adäquate Datenschutzvorkehrungen.*

Nach den Terroranschlägen vom 11. September 2001 in New York und Washington und den Erfahrungen aus dem Sommerhochwasser 2002 ist die Thematik des Bevölkerungs- und Zivilschutzes in Deutschland wieder stärker in den Vordergrund gerückt. Mit der „Neuen Strategie zum Schutz der Bevölkerung in Deutschland“ (Beschluss der Innenministerkonferenz vom 5./6. Juni 2002) hatten sich Bund und Länder auf eine verbesserte Zusammenarbeit verständigt. Bei der Katastrophenhilfe durch den Bund stehen Fragen der Koordinierung und des Managements von Engpassressourcen im Vordergrund. In der Folge wurde 2004 das BBK durch das BBK-Gesetz als Bundesoberbehörde im Geschäftsbereich des BMI gegründet.

Da zum Nachweis personeller Ressourcen datenschutzrelevante personenbezogene Daten gespeichert werden, habe ich im Rahmen meiner Beteiligung am Gesetzgebungsverfahren entsprechende Anregungen gegeben. Ich habe ferner das BBK gebeten, die praktische Ausgestaltung seiner Datenschutzvorkehrungen insgesamt in einem Datenschutzkonzept darzulegen. An diesem Konzept wird noch gearbeitet.

Parallel habe ich mich bei einem Beratungs- und Kontrollbesuch beim BBK kundig gemacht, wie die Behörde mit personenbezogenen Daten umgeht und insofern bei ihren weiteren Arbeiten unterstützt werden kann. Weitere Besuche werden sich auf die verschiedenen relevanten Fachbereiche des BBK erstrecken und voraussichtlich im Laufe der ersten Jahreshälfte 2011 zum Abschluss kommen. Die europäische und internationale Einbindung des BBK bedarf hierbei einer besonderen datenschutzbezogenen Evaluation.

Das THW stellt mit 80 000 freiwilligen ehrenamtlichen Helferinnen und Helfern einen großen Teil des technisch orientierten Hilfeleistungspotenzials für die Gefahrenabwehr in Deutschland. Angesichts der großen Helferzahl und der vielfältigen Vernetzung durch Einbindung in die örtliche Gefahrenabwehr einerseits sowie in europäische und internationale Einsätze andererseits, die den raschen Zugriff auf gespeicherte Helferdaten und deren Weitergabe erfordern, hat hier auch der Datenschutz eine Bedeutung. Ich habe daher das THW gebeten, ein Daten-

schutzkonzept zu erstellen. Dieses liegt in einer ersten Fassung vor, bedarf aber noch der Ergänzung.

Auch beim THW habe ich mit Beratungs- und Kontrollbesuchen, zunächst bei der THW-Leitung in Bonn, begonnen. Angesichts des hierarchischen Aufbaus des THW als bundeseigene Verwaltung über die Länder- bis auf die Ortsebene werden die Besuche fortgesetzt. Sie sollen bis Mitte 2011 abgeschlossen werden.

### 8.7 Forschungsprojekt Doping des Bundesinstituts für Sportwissenschaft

*Ein Forschungsprojekt des Bundesinstituts für Sportwissenschaft (BISp) beschäftigt sich mit Doping unter historisch-soziologischen und ethischen Aspekten. Für die Zeit von 1950 bis 1990 widmet sich das Projekt Westdeutschland, danach ganz Deutschland. Dass dabei auch persönliche Daten in den Blick geraten, liegt nahe.*

Das BISp hat in das Projekt auch die Humboldt-Universität zu Berlin und die Westfälische Wilhelms-Universität in Münster eingebunden und lässt es durch einen projektbezogenen wissenschaftlichen Beirat begleiten. Die datenschutzbezogene Beratung beider Universitäten erfolgt durch meine zuständigen Länderkollegen in Nordrhein-Westfalen und Berlin, während das BISp selbst von mir beraten wird.

Bereits von Beginn an sieht das projektbezogene Datenschutzkonzept vor, dass der wissenschaftliche Beirat nur anonymisierte Daten erhält. Dies begrüße ich ebenso wie die Aufgeschlossenheit des BISp, meine bisherigen Datenschutzempfehlungen zu weiteren Konzeptdetails umzusetzen.

Als Datenquellen des Projekts dienen öffentlich zugängliche Informationen, Archive und Zeitzeugenbefragungen. Das Konzept stellt klar, dass es sich hierbei um personenbezogene Daten handelt und dass besondere Arten personenbezogener Daten nach § 3 Absatz 9 BDSG, wie etwa Gesundheitsangaben, nicht erhoben werden sollen. Ebenfalls nicht erhoben werden Daten Dritter in den Befragungen der Zeitzeugen. Ihre unverzügliche Löschung nach versehentlicher Erhebung ist vorgegeben.

Gleichfalls wird die Beachtung der einschlägigen datenschutzrechtlichen Regelungen bei der Erhebung, Verarbeitung und Nutzung von Daten für Zwecke der wissenschaftlichen Forschung betont. Die Gebote zur Pseudonymisierung und Anonymisierung der zur wissenschaftlichen Forschung verwendeten Daten und die einschlägigen Löschungsvorschriften werden im Konzept berücksichtigt. Die Beratung hinsichtlich technisch-organisatorischer Prozesse zur Abrundung der Vorkehrungen zur Datensicherheit dauert noch an.

Angesichts der Projektstruktur müssen Verträge zur Auftragsdatenverarbeitung zwischen dem BISp und den Universitäten abgeschlossen werden. Die entsprechenden Vertragsentwürfe stehen grundsätzlich im Einklang mit § 11 BDSG, so dass ich hier nur geringfügige Hinweise zur Verbesserung weniger Formulierungen geben musste (vgl. zu § 11 BDSG auch Nr. 2.4).

Der Austausch von Informationen zwischen dem BISp, den genannten Universitäten und projektexternen Forscherinnen und Forschern anderer Universitäten erfolgte nach Angaben des BISp bisher ohne personenbezogene Daten. Das BISp hat versichert, dass im Fall des künftigen Austauschs personenbezogener Daten Einvernehmen mit den Beteiligten herrsche, dass dies so wenig wie möglich und unter Beachtung strikter Zweckbindung geschehen solle.

### 8.8 Fortbildungsangebot der BAköV für behördliche Datenschutzbeauftragte

*Die Bundesakademie für öffentliche Verwaltung plant einen Fortbildungsgang für behördliche Datenschutzbeauftragte mit abschließendem Zertifikatserwerb. Eine solche Aus- bzw. Fortbildung halte ich mit Blick auf die gesetzlichen Anforderungen an die Fachkunde des Datenschutzbeauftragten für sehr wichtig und unterstütze sie.*

Nach § 4f Absatz 2 Satz 1 BDSG darf zum Beauftragten für den Datenschutz nur bestellt werden, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Was konkret hierunter zu verstehen ist, wird im Gesetz nicht näher ausgeführt. Es ist weder ein bestimmter Ausbildungsgang noch ein bestimmter Abschluss vorgeschrieben. Wie man sich die erforderliche Fachkunde aneignet, bleibt also jedem selbst überlassen. Dies führt in der Praxis zu qualitativen Unterschieden bei der Auswahl und der Fortbildung und ist wegen der gestiegenen Anforderungen an die Funktion des Datenschutzbeauftragten unbefriedigend.

Aus diesem Grund habe ich es sehr begrüßt, dass die Bundesakademie für öffentliche Verwaltung (BAköV) beabsichtigt, ihr Fortbildungsangebot um einen Fortbildungsgang für behördliche Datenschutzbeauftragte mit abschließendem Zertifikatserwerb zu erweitern. Ziel dieses Lehrgangs, der zunächst nur Bediensteten der Bundesverwaltung angeboten werden wird, soll es sein, Mitarbeiterinnen und Mitarbeiter für die Tätigkeit als behördliche Datenschutzbeauftragte zu befähigen, zu zertifizieren und weiter fortzubilden.

Ich bin deshalb der Bitte der BAköV, Vorbereitung und Planung eines solchen Fortbildungslehrgangs zu unterstützen, gerne nachgekommen. In mehreren Besprechungen wurden die inhaltlichen Schwerpunkte für die Fortbildung von Datenschutzbeauftragten festgelegt sowie ein entsprechendes Rahmenkonzept entwickelt.

Das Konzept sieht vor, die Ausbildung modular aufzubauen und flexibel zu gestalten, indem ein individueller Lehrpfad (Festlegung der zu besuchenden Seminare) erstellt werden kann. Den individuellen Vorkenntnissen und Aufgabenfeldern soll ebenfalls Rechnung getragen werden. Ein geplanter Selbsteinschätzungstest soll es den Teilnehmer ermöglichen, zunächst ihren persönlichen Fortbildungsbedarf zu ermitteln. In dem für die Zertifizierung erforderlichen praktischen Teil des Fortbildungsangebots sind eine Projektarbeit, ein Workshop sowie die Abschlussprüfung vorgesehen. Begleitend zur Fortbildung soll ein den inhaltlichen Themen des Basislehrgangs angepasstes Handbuch (Repetitorium) erstellt werden.

Auf der Grundlage des mit mir gemeinsam erstellten Rahmenkonzepts hat die BAköV inzwischen Ausschreibungen für die Erstellung eines Feinkonzepts, des Selbsteinschätzungstest, eines Fragenpools für die Abschlussprüfung sowie des Handbuchs veranlasst.

## 8.9 Qualifizierung und Freistellung behördlicher Datenschutzbeauftragter

*Die verantwortliche Tätigkeit der Beauftragten für den Datenschutz erfordert nicht nur ein hohes Maß an Fachkunde. Ihre gesetzlich vorgeschriebene Unabhängigkeit ist nur gewährleistet, wenn sie angemessen von anderen Aufgaben entlastet werden und genügend Zeit für die Wahrnehmung ihres Amtes haben. Hierzu fehlen jedoch konkrete Vorgaben.*

Der Institution des durch § 4f BDSG vorgesehenen behördlichen Datenschutzbeauftragten kommt bei der Einhaltung des Datenschutzes und der Umsetzung datenschutzrechtlicher Bestimmungen besondere Bedeutung und Verantwortung zu. Diese Aufgabe erfordert ein hohes Maß an Fachkunde sowie eine unabhängige und organisatorisch herausgehobene Stellung.

Das BDSG erläutert den Begriff der erforderlichen Fachkunde zwar nicht näher, grundlegende Kenntnisse zum Inhalt und zur rechtlichen Anwendung des Bundesdatenschutzgesetzes sowie zu spezialgesetzlichen datenschutzrelevanten Regelungen, zur Informations- und Kommunikationstechnologie und zu Datensicherheitsanforderungen nach § 9 BDSG müssen jedoch gewährleistet sein. Soweit er nicht bereits darüber verfügt, muss sich der behördliche Datenschutzbeauftragte die entsprechenden Kenntnisse vor allem durch den Besuch von Fortbildungsseminaren mit Unterstützung seiner Dienststelle aneignen.

In der am 1. September 2010 in Kraft getretenen BDSG-Novelle (vgl. Nr. 2.2) wurde ein Anspruch auf Teilnahme an Schulungs- und Fortbildungsveranstaltungen sowie Übernahme der Kosten durch die verantwortliche Stelle festgeschrieben. Solche Datenschutzfortbildungen haben bisher in erster Linie private Anbieter durchgeführt. Deshalb begrüße ich, dass die Bundesakademie für öffentliche Verwaltung den Beschäftigten in der Bundesverwaltung demnächst neben dem Grundseminar „Datenschutz“ einen Fortbildungsgang für behördliche Datenschutzbeauftragte mit abschließendem Zertifikatserwerb anbieten will (vgl. o. Nr. 8.8).

Beim regelmäßigen Erfahrungsaustausch mit den Datenschutzbeauftragten der obersten Bundesbehörden (vgl. u. Nr. 14.2) habe ich mich immer wieder über deren Situation informiert, insbesondere über Arbeitsanfall, die organisatorischen Zuordnung sowie die Unterstützung durch ihre Dienststelle. Die Betroffenen können in vielen Fällen ihre Aufgaben nur neben ihrer eigentlichen Tätigkeit ausüben und sind deshalb nicht in der Lage, den an ihr Amt gestellten Anforderungen – auch bei größtem persönlichem Einsatz – in vollem Umfang gerecht zu werden. Dies ist umso unbefriedigender, als die steigende Bedeutung des Datenschutzes immer mehr Aufgaben und Anforderungen an die Datenschutzbeauftragten mit sich bringt. Von Seiten der Datenschutzbeauftragten wurde ich daher gebeten, Richtlinien oder Empfehlungen zu geben, sowohl zur Ausgestaltung der Kontrolltätigkeit als auch zur Ermittlung des Freistellungsbedarfs. Auch gesetzliche Regelungen werden teilweise gefordert.

Nach § 4f Absatz 5 Satz 1 BDSG haben die verantwortlichen Stellen den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen. Von entscheidender Bedeutung ist hier eine angemessene Entlastung von möglicherweise übertragenen anderen Aufgaben, auch wenn ein gesetzlicher Freistellungsanspruch für den Datenschutzbeauftragten nicht gegeben ist. Alle Rechte und Befugnisse können dem Datenschutzbeauftragten nur von Nutzen sein, wenn er ausreichend Zeit für die Wahrnehmung seiner Aufgabe hat.

In meinem 20. TB (Nr. 2.4) hatte ich bereits einmal den Gesetzgeber aufgefordert, eine adäquate gesetzliche Freistellungsregelung in das BDSG aufzunehmen. Die Bundesregierung ist diesem Vorschlag nicht gefolgt, hat aber ausdrücklich anerkannt, dass aus der Unterstützungspflicht der Dienststelle auch die Pflicht zur teilweisen oder völligen Freistellung von anderen Aufgaben folgt (vgl. 21. TB Nr. 2.6 sowie Kasten a zu Nr. 8.9).

Da zahlreiche Dienststellen offensichtlich den Aufgabenbereich und Arbeitsanfall der Datenschutzbeauftragten nicht richtig kennen oder einschätzen, werde ich mich verstärkt bemühen, durch Aufklärung Abhilfe zu schaffen. Allgemeingültige Aussagen zur Notwendigkeit einer Freistellung oder zur Anzahl des erforderlichen Hilfspersonals lassen sich nur schwer treffen. Bei größeren Behörden mit zahlreichen Beschäftigten und PC-Arbeitsplätzen oder auch besonders umfangreicher oder sensibler personenbezogener Datenverarbeitung kann die Bestellung eines hauptberuflichen Datenschutzbeauftragten durchaus geboten sein. Allerdings kann die Anzahl der Beschäftigten alleine nicht ausschlaggebend sein. Es kommt vielmehr auf den Umfang und die Sensibilität der Daten an. Gleichwohl werde ich prüfen, ob und inwieweit den Behörden des Bundes Empfehlungen zu den Kapazitätsanforderungen für behördliche Datenschutzbeauftragte gegeben werden können.

Der Düsseldorfer Kreis, ein Koordinierungsgremium aller Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich, hat mit Blick auf die ähnliche Problematik bei den betrieblichen Datenschutzbeauftragten in der Privatwirtschaft in seinem Beschluss vom 24./25. November 2010 „Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Absatz 2 und 3 Bundesdatenschutzgesetz“ (Kasten b zu Nr. 8.9) eine Art Leitbild für das Amt des Beauftragten für den Datenschutz erstellt. Dieser Beschluss könnte als Grundlage für eine vergleichbare Empfehlung für die behördlichen Datenschutzbeauftragten in den Bundesbehörden dienen.

Kasten a zu Nr. 8.9

**Auszug aus der Stellungnahme der Bundesregierung zum 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 26 Absatz 1 des Bundesdatenschutzgesetzes – Bundestagsdrucksache 15/5252 –**

**Zu Nr. 2.4 – Stärkung der behördlichen Datenschutzbeauftragten**

Der BfD fordert eine gesetzliche Freistellung der behördlichen Datenschutzbeauftragten von ihren dienstlichen Verpflichtungen entsprechend den Regelungen für die Mitglieder der Personalvertretung oder die Gleichstellungsbeauftragte.

Nach § 4f Absatz 1 BDSG haben öffentliche und nicht-öffentliche Stellen einen Beauftragten für den Datenschutz zu bestellen. Aufgabe dieses Datenschutzbeauftragten ist es, innerhalb der verantwortlichen Stelle auf die Einhaltung der Vorschriften über den Datenschutz hinzuwirken (§ 4g Absatz 1 BDSG). Nach § 4f Absatz 5 BDSG hat die öffentliche oder nicht-öffentliche Stelle den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Wenn auf Grund der Größe der verantwortlichen Stelle oder des Umfangs, in der diese personenbezogene Daten verarbeitet, die Aufgaben des Beauftragten für den Datenschutz einen solchen Umfang annehmen, dass er diese zeitlich und organisatorisch nicht mehr mit anderen Aufgaben vereinbaren kann, folgt aus der Unterstützungspflicht auch die Pflicht, ihn entsprechend (teilweise oder völlig) von anderen Aufgaben freizustellen. Dies ist bei vielen Bundesbehörden, wie der BfD zutreffend feststellt, der Fall. Im Ergebnis unterscheidet sich die Regelung der §§ 4f, 4g BDSG daher nicht von den Freistellungsregelungen der §§ 18 Absatz 2 Bundesgleichstellungsgesetz oder 46 Absatz 3 Bundespersonalvertretungsgesetz, die ebenfalls eine Freistellung nur verlangen, wenn dies nach Art und Umfang der Dienststelle zur ordnungsgemäßen Aufgabenerfüllung erforderlich ist.

§ 4f Absatz 5 BDSG gibt den verantwortlichen Stellen und deren Datenschutzbeauftragten allerdings mehr organisatorische Freiheiten an die Hand. So kann es für die Arbeit des Beauftragten für den Datenschutz nützlicher sein, wenn dieser zwar andere Aufgaben in Zugleichfunktion behält, dafür aber auf Mitarbeiterressourcen und damit zum Beispiel auch auf bestimmtes technisches oder juristisches Know-how zurückgreifen kann. Eine solche flexible und unbürokratische Lösung ist einer starren Freistellungspflicht nach dem Vorbild des Personalvertretungsrechts vorzuziehen. Insbesondere für kleine und mittlere Unternehmen könnte eine Pflicht, nicht nur einen Datenschutzbeauftragten zu bestellen, sondern diesen auch von anderen Aufgaben freizustellen, existenzbedrohende Auswirkungen haben.

Kasten b zu Nr. 8.9

**Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 24./25. November 2010**

**Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Absatz 2 und 3 Bundesdatenschutzgesetz (BDSG)**

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bei der Kontrolle verantwortlicher Stellen festgestellt, dass Fachkunde und Rahmenbedingungen für die Arbeit der Beauftragten für den Datenschutz (DSB) in den verantwortlichen Stellen angesichts zunehmender Komplexität automatisierter Verfahren zum Umgang mit personenbezogenen Daten nicht durchgängig den Anforderungen des BDSG genügen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass die Aus- und Belastung der DSB maßgeblich beeinflusst wird durch die Größe der verantwortlichen Stelle, die Anzahl der zu betreuenden verantwortlichen Stellen, Besonderheiten branchenspezifischer Datenverarbeitung und den Grad der Schutzbedürftigkeit der zu verarbeitenden personenbezogenen Daten. Veränderungen bei den vorgenannten Faktoren führen regelmäßig zu einer proportionalen Mehrbelastung der DSB.

Nachfolgende Mindestanforderungen sind zu gewährleisten:

**I. Erforderliche Fachkunde gemäß § 4f Absatz 2 Satz 1 BDSG**

§ 4 f Absatz 2 Satz 1 BDSG legt fest, dass zum Beauftragten für den Datenschutz (DSB) nur bestellt werden darf, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Weitere Ausführungen dazu enthält das Gesetz nicht. Vor dem Hintergrund der gestiegenen Anforderungen an die Funktion des DSB müssen diese mindestens über folgende datenschutzrechtliche und technisch-organisatorische Kenntnisse verfügen:

1. Datenschutzrecht allgemein – unabhängig von der Branche und der Größe der verantwortlichen Stelle
   - Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Mitarbeiter der verantwortlichen Stelle und

- umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die verantwortlichen Stellen einschlägigen Regelungen des BDSG, auch technischer und organisatorischer Art,
- Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach § 9 BDSG.

2. Branchenspezifisch – abhängig von der Branche, Größe oder IT-Infrastruktur der verantwortlichen Stelle und der Sensibilität der zu verarbeitenden Daten
   - Umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind,
   - Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen, etc.),
   - betriebswirtschaftliche Grundkompetenz (Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management, Marketing etc.),
   - Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle (Aufbau- und Ablaufstruktur bzw. Organisation der verantwortlichen Stelle) und
   - Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle (z. B. Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat etc.).

Grundsätzlich müssen die erforderlichen rechtlichen, technischen sowie organisatorischen Mindestkenntnisse **bereits zum Zeitpunkt der Bestellung** zum DSB im ausreichenden Maße vorliegen. Sie können insbesondere auch durch den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer Prüfung erlangt sein. Um eventuell zu Beginn der Bestellung noch bestehende Informationsdefizite auszugleichen, empfiehlt sich der Besuch von geeigneten Fortbildungsveranstaltungen. Der Besuch solcher Veranstaltungen ist auch nach der Bestellung angezeigt, um auf dem aktuellen, erforderlichen Informationsstand zu bleiben, und um sich Kenntnisse über die sich ändernden rechtlichen und technischen Entwicklungen anzueignen.

**II. Anforderungen an die Unabhängigkeit der/des Beauftragten gem. § 4f Absatz 3 BDSG**

Gemäß § 4f Absatz 3 Satz 2 BDSG sind DSB in Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Um die Unabhängigkeit der DSB zu gewährleisten, sind eine Reihe betriebsinterner organisatorischer Maßnahmen erforderlich:

1. DSB sind dem Leiter/der Leiterin der verantwortlichen Stelle organisatorisch unmittelbar zu unterstellen (§ 4f Absatz 3 Satz 1 BDSG). Sie müssen in der Lage sein, ihre Verpflichtungen ohne Interessenkonflikte erfüllen zu können. Dieses ist durch entsprechende Regelungen innerhalb der verantwortlichen Stelle bzw. vertragliche Regelungen sicher zu stellen und sowohl innerhalb der verantwortlichen Stelle als auch nach außen hin publik zu machen. Den DSB ist ein unmittelbares Vortragsrecht beim Leiter der Stelle einzuräumen.
2. DSB dürfen wegen der Erfüllung ihrer Aufgaben in Hinblick auf ihr sonstiges Beschäftigungsverhältnis, auch für den Fall, dass die Bestellung zum DSB widerrufen wird, nicht benachteiligt werden (vgl. § 4f Absatz 3 Satz 3 ff BDSG).Analog muss bei der Bestellung von externen DSB der Dienstvertrag so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet wird. § 4f Absatz 3 BDSG schränkt insoweit die grundsätzliche Vertragsfreiheit ein. Empfohlen wird grundsätzlich eine Mindestvertragslaufzeit von 4 Jahren, bei Erstverträgen wird wegen der Notwendigkeit der Überprüfung der Eignung grundsätzlich eine Vertragslaufzeit von 1 – 2 Jahren empfohlen.
3. Datenschutzbeauftragte sind zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit sie nicht davon durch die Betroffenen befreit wurden. Dies gilt auch gegenüber der verantwortlichen Stelle und deren Leiter (§ 4f Absatz 4 BDSG).

**III. Erforderliche Rahmenbedingungen innerhalb der verantwortlichen Stelle zur Fachkunde und Unabhängigkeit des DSB**

1. Die Prüfpflichten der DSB (vgl. § 4g BDSG) setzen voraus, dass ihnen die zur Aufgabenerfüllung erforderlichen Zutritts- und Einsichtsrechte in alle betrieblichen Bereiche eingeräumt werden.
2. DSB müssen in alle relevanten betrieblichen Planungs- und Entscheidungsabläufe eingebunden werden. Sie führen das Verfahrensverzeichnis (§ 4g Absatz 2 BSDG) und haben hierfür die erforderlichen Unterlagen zu erhalten.

3. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde haben die verantwortlichen Stellen den DSB die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Bei der Bestellung von externen DSB kann die Fortbildung Bestandteil der vereinbarten Vergütung sein und muss nicht zusätzlich erbracht werden.
4. Internen DSB muss die erforderliche Arbeitszeit zur Erfüllung ihrer Aufgaben und zur Erhaltung ihrer Fachkunde zur Verfügung stehen. Bei Bestellung eines externen DSB muss eine bedarfsgerechte Leistungserbringung gewährleistet sein. Sie muss in angemessenem Umfang auch in der beauftragenden verantwortlichen Stelle selbst erbracht werden. Ein angemessenes Zeitbudget sollte konkret vereinbart und vertraglich festgelegt sein.
5. Die verantwortlichen Stellen haben DSB bei der Erfüllung ihrer Aufgaben insbesondere durch die zur Verfügung Stellung von Personal, Räumen, Einrichtung, Geräten und Mitteln zu unterstützen (§ 4f Absatz 5 BDSG).

### 8.10 Neuerungen im Strafprozess- und Strafvollzugsrecht

*Datenschutzrelevante Gesetzesänderungen betrafen den Schutz von Berufsgeheimnisträgern im Ermittlungsverfahren sowie die Einführung der elektronischen Aufenthaltsüberwachung für entlassene Straftäter.*

Bereits im Gesetzgebungsverfahren zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen in der StPO hatte ich kritisiert, dass der Schutz der Berufsgeheimnisträger bei dieser Reform nicht hinreichend berücksichtigt wurde (vgl. 21. TB Nr. 6.1, 22. TB Nr. 5.1). Durch die seinerzeit neu eingeführte Regelung des § 160a StPO wurde das Zeugnisverweigerungsrecht Geistlicher, Strafverteidiger und Abgeordneter einem absoluten Schutz vor strafprozessualen Ermittlungsmaßnahmen unterstellt; für die übrigen zeugnisverweigerungsberechtigten Berufsgeheimnisträger wie etwa Rechtsanwälte oder Ärzte wurde nur ein relatives, d. h. von einer Verhältnismäßigkeitsprüfung im Einzelfall abhängiges Beweiserhebungs- und -verwertungsverbot vorgesehen. Erfreulicherweise hat die Bundesregierung nunmehr damit begonnen, diese Schlechterstellung bestimmter Berufsgeheimnisträger zumindest teilweise zu beseitigen, und ein Gesetz auf den Weg gebracht, das den absoluten Schutz auf sämtliche Rechtsanwälte erstreckt (Gesetz zur Stärkung des Schutzes von Vertrauensverhältnissen zu Rechtsanwälten im Strafprozessrecht vom 22. Dezember 2010, BGBl. I S. 2261). Dieses Vorhaben habe ich gegenüber dem BMJ ausdrücklich begrüßt. Zugleich habe ich meine Forderung wiederholt, für sämtliche zeugnisverweigerungsberechtigten Berufsgeheimnisträger ein einheitliches und hohes Schutzniveau zu schaffen. Die Bundesregierung hat angekündigt, die Einbeziehung weiterer Berufsgeheimnisträger in den absoluten Schutz zu prüfen. Ich werde die weitere Entwicklung aufmerksam verfolgen.

Ein besonderes Augenmerk werde ich auch auf die technische Realisierung der sog. elektronischen Aufenthaltsüberwachung richten, die durch das Gesetz zur Neuordnung des Rechts der Sicherungsverwahrung vom 22. Dezember 2010 (BGBl. I S. 2300) als neues Instrument der Führungsaufsicht zur Überwachung von weiterhin rückfallgefährdeten, aber in die Freiheit zu entlassenden Straftätern eingeführt worden ist. Bereits im Gesetzgebungsverfahren habe ich darauf hingewiesen, dass die elektronische Aufenthaltsüberwachung einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt. Sie trägt Elemente einer unzulässigen Rundumüberwachung in sich, die zur Erstellung umfassender Bewegungs- und Persönlichkeitsprofile führen könnte. Bei der technischen Ausgestaltung der Überwachung ist daher insbesondere sicherzustellen, dass der Aufenthaltsort nur zweckbezogen und nicht jederzeit oder gar fortlaufend kontrolliert werden kann und ein unberechtigter Zugriff Dritter auf die erhobenen Daten verhindert wird. Außerdem ist zum Schutz der Privatsphäre des Betroffenen zu gewährleisten, dass innerhalb der Wohnung keine raumgenaue Ortung stattfindet. Ich befürworte die Empfehlung in der Gesetzesbegründung (Bundestagsdrucksache 17/3403 S. 19), mangels einschlägiger praktischer Erfahrungen in Deutschland zunächst in Pilotprojekten zu klären, welche technischen Vorkehrungen zu treffen und welche Geräte – mit welchen Messgenauigkeiten – im Einzelnen einzusetzen sind.

## 9 Finanzwesen

### 9.1 Steuerdaten-CD – Kein Datenschutz nach Kassenlage!

*Die Diskussion um den Ankauf von Steuerdaten-CD zweifelhafter Herkunft hat das Spannungsfeld zwischen den Möglichkeiten und Grenzen rechtsstaatlichen Handelns offenbart. Ich halte eine spezielle Rechtsgrundlage für nötig, um die widerstreitenden Interessen und Rechtsgüter in einen angemessenen Ausgleich zu bringen.*

Die Diskussion, ob der Staat aus „zwielichtigen Quellen“ stammende CD mit Datensätzen über mutmaßliche Steuerhinterzieher ankaufen soll, wurde sowohl unter Datenschützern als auch in der politisch interessierten Öffentlichkeit kontrovers geführt. Anlass hierfür war das Angebot eines Datendealers, der illegal beschaffte Datensätze über Kunden einer Schweizer Bank dem deutschen Staat angeboten hatte. Die Befürworter eines Ankaufs hatten kein Verständnis dafür, dass sich der deutsche Fiskus aufgrund datenschutzrechtlicher Bedenken an der Herkunft der Daten dieser nicht bedienen könne. Unter dem Deckmantel des Datenschutzes dürften solche Daten nicht zur Verheimlichung von Steuerhinterziehung geschützt werden. Daher sei die deutsche Steuerverwaltung auch nicht daran gehindert, mit den Informanten zusammenzuarbeiten.

Ich habe mich trotzdem gegen den Ankauf von Datensätzen ausgesprochen, soweit sie aus einer illegalen Quelle stammen. Ein Rechtsstaat zeichnet sich dadurch aus, dass

sein Handeln an Recht und Gesetz gebunden ist. Die relevanten Vorgaben für behördliche Ermittlungen finden sich insbesondere in der Strafprozessordnung, die einen heimlichen Zugriff auf informationstechnische Systeme gerade nicht erlaubt. Auch die für die Steuerfahnder geltenden Vorschriften der Abgabenordnung erlauben nicht das heimliche Eindringen in fremde Computer und die Sichtung der dort gespeicherten Daten, um Hinweise auf Steuerhinterzieher zu suchen. Offenbar hat der Informant von ihm angebotene Daten auf diese oder vergleichbar rechtswidrige Weise erlangt. Unter Verstoß gegen Datenschutzvorschriften erlangte Daten bleiben aber rechtswidrig, auch wenn sie für einen „guten" Zweck verwandt werden sollen. Der Rechtsstaat darf sich der ihm durch das Recht auferlegten Grenzen nicht dadurch entledigen, indem er auf rechtswidriges Handeln Dritter setzt.

Eine besondere Problematik liegt auch in den Konsequenzen, die sich aus der Belohnung von „Datendieben" ergeben können. Wenn der Staat beim Ankauf einer CD mit illegal erlangten Datensätzen dem Informanten Geld gibt, anstatt ihn für sein strafbares Handeln zur Rechenschaft zu ziehen (und eventuell auszuliefern), stellt sich die Frage, ob er nicht zumindest mittelbar den Diebstahl vertraulicher personenbezogener Daten fördert.

Der Ankauf einer aus illegalen Quellen stammenden Steuerdaten-CD stellt aufgrund seiner Eigenart eine besondere Ermittlungsmaßnahme dar, die meiner Ansicht nach allenfalls auf der Grundlage einer besonderen – aber bei derzeitiger Rechtslage nicht erkennbaren – Ermächtigung zulässig sein kann. Behörden in einem Rechtsstaat müssen in klarer und nachvollziehbarer Weise ihre Ermittlungen führen. Dazu zählt auch Transparenz hinsichtlich der Frage, auf welchem Wege Informationen in die Hände der Steuerverwaltung gelangt sind.

Ich habe mich deshalb dafür ausgesprochen, auf Bundesebene konkrete gesetzliche Regelungen zum Umgang mit Angeboten von Datensätzen zu Steuersündern zu schaffen. Dabei ist der Gesetzgeber aufgefordert, die widerstreitenden Interessen und Rechtsgüter in einen angemessenen Ausgleich zu bringen. Unabhängig davon darf ein Ankauf solcher Datensätze aber allenfalls eine *ultima ratio* darstellen. Die Steuerbehörden müssen zuvor die verfügbaren ihm zu Gebote stehenden Wege der Informationserlangung ausgeschöpft haben. Dazu zählen insbesondere der Informationsaustausch mit ausländischen Finanzbehörden sowie die Ausschöpfung der Möglichkeiten der Rechtshilfe (vgl. Nr. 9.7). Zudem dürfen etwaige gesetzliche Regelungen nicht das Geschäftsmodell der illegalen Datenbeschaffung oder des illegalen Datenhandels fördern. Im Übrigen teile ich die Auffassung, dass sich – losgelöst von der vorliegenden Thematik – die Frage des Umgangs mit Daten aus „zwielichtigen Quellen" für die Strafverfolgungsbehörden aufgrund des technischen Fortschritts vermehrt stellen wird. Dies spricht ebenfalls für die Schaffung einer spezialgesetzlichen Regelung.

Im Zusammenhang mit den Überlegungen zu einer Rechtsgrundlage bedarf meines Erachtens auch die Frage nach der Verwertung der durch den Ankauf erlangten Informationen einer weiteren Erörterung. Inzwischen hat das Bundesverfassungsgericht entschieden, dass der für eine Wohnungsdurchsuchung erforderliche Anfangsverdacht auf Daten gestützt werden kann, die ein Informant aus Liechtenstein auf einer CD-ROM an den Bundesnachrichtendienst verkauft hatte (BVerfG, Beschluss vom 9. November 2010, 2 BvR 2101/09). Damit ist allerdings die Frage der Zulässigkeit des Erwerbs derartiger Daten nicht abschließend geklärt.

## 9.2 Die Macht der Steuer-Identifikationsnummer

*Durch die Steuer-Identifikationsnummer (Steuer-ID) werden alle Bundesbürger zentral durch den Staat erfasst. Erweiterungen des Datenbestandes oder Vernetzungen verschiedener auf der Steuer-ID basierender Datenpools bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung.*

Seit der Einführung der Steuer-ID habe ich auf die Gefahr hingewiesen, aus diesem Merkmal könne sich ein Personenkennzeichen entwickeln, mit dem andere Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden können (s. 22. TB Nr. 9.1). Diese Gefahr besteht weniger darin, dass die Steuer-ID in ein allgemeines Personenkennzeichen umgewandelt wird. Vielmehr ist zu befürchten, dass deren Verwendungsmöglichkeiten schrittweise erweitert werden, was im Ergebnis auf dasselbe hinausläuft.

Die jüngsten Entwicklungen bestätigen leider meine Bedenken. Mit dem Jahressteuergesetz 2010 hat die Steuer-ID zusätzliche neuen Funktionen erhalten, durch die – wie vom Gesetzgeber gewünscht – der Vollzug der Steuergesetze und damit eine gleichmäßige Besteuerung besser gewährleistet werden. Der Staat erhält hierdurch aber auch neue Möglichkeiten, unter der Steuer-ID verschiedenste Daten zu seinen Bürgern in einer zentralen Datenbank zu speichern. Problematisch ist aber vor allem, dass die Steuer-ID verstärkt von nicht-öffentlichen Stellen erhoben und verarbeitet wird.

Dies geschieht beispielsweise durch die mit dem „Bürgerentlastungsgesetz Krankenversicherung" eingeführten Regelungen nach § 10 Absatz 2 und Absatz 2a EStG. Diese bestimmen im Zusammenhang mit der steuerlichen Geltendmachung von Vorsorgeaufwendungen durch die Versicherten die Erhebung und Verarbeitung der Steuer-ID durch die privaten Krankenversicherungsunternehmen. Wie zahlreiche Eingaben belegen, befürchten die Betroffenen eine Entwicklung zum „gläsernen Steuerbürger". Besonders kritisiert wird dabei, dass eine steuerliche Berücksichtigung der Vorsorgeaufwendungen in vollem Umfang nur möglich ist, wenn die Betroffenen der Erhebung und Verarbeitung der Steuer-ID durch die Krankenversicherungsunternehmen zustimmen.

Eine wirksame Einwilligung nach § 4a Absatz 1 Satz 1 BDSG setzt jedoch eine freie Entscheidung des Betroffenen voraus, die wiederum auf einer echten Wahlmöglichkeit beruhen muss, die im konkreten Fall nicht besteht. Ich habe mich daher gegenüber dem Bundesministerium der Finanzen (BMF) dafür eingesetzt, den Steuerpflichti-

gen alternative Möglichkeiten zu eröffnen, die gemachten Vorsorgeaufwendungen nachzuweisen, etwa durch Vorlage von entsprechenden Bescheinigungen beim Finanzamt. Zu meinem Bedauern ist das BMF meiner Empfehlung bislang nicht gefolgt.

Weiter ist problematisch, dass die Betroffenen wegen der vielfältigen Verwendungsmöglichkeiten der Steuer-ID durch unterschiedlichste Stellen nicht ohne Weiteres Kenntnis davon erhalten, welche Daten bei welchen Stellen darunter gespeichert werden. Die Folge wäre eine „schleichende", von den Betroffenen unbemerkte Datenmehrung. Kritisch sehe ich auch, dass der Gesetzgeber durch die Einführung neuer Rechtsgrundlagen die Speicherung weiterer steuerrechtlich relevanter Daten unter der Steuer-ID veranlassen kann. Dies ist beispielsweise mit Blick auf die Speicherung von lohnsteuerrelevanten Daten nach § 39e EStG bereits geschehen (s. Nr. 9.3). Da das Steuerrecht in nahezu alle Lebensbereiche hineinreicht, könnten dabei sehr weit reichende Datensätze entstehen. Diese Datenpools können möglicherweise auch Rückschlüsse auf Tatsachen zulassen, die keinen unmittelbaren steuerlichen Bezug haben.

Meine Bedenken werden auch vom Finanzgericht Köln geteilt, das in einem Musterverfahren die Rechtmäßigkeit der auf der Rechtsgrundlage von §§ 139a und 139b Abgabenordnung erhobenen Steuer-ID geprüft hat (FG Köln, Urteil vom 7. Juli 2010, 2 K 3093/08). Zwar hat das Gericht „bedeutende Zweifel" an der Verfassungsmäßigkeit der Steuer-ID, diese reichten aber nicht für die „volle Überzeugungsbildung" bezüglich einer Verfassungswidrigkeit aus, sodass das Bundesverfassungsgericht letztlich nicht mit dieser Frage befasst wurde.

Angesichts der Sensibilität der Daten und der möglichen Gefährdungen durch die Nutzung automatischer Datenverarbeitungen im Zusammenhang mit der Steuer-ID habe ich bereits frühzeitig auf die erforderliche Absicherung der Datenbank durch ein umfassendes verfahrensspezifisches IT-Sicherheitskonzept hingewiesen. Dieses wurde mir erst nach einer formalen Beanstandung nach § 25 Absatz 1 BDSG vom BMF vorgelegt. Ich prüfe derzeit die umfangreichen Unterlagen und beabsichtige, den Umgang mit den Steuerdaten im Rahmen eines Beratungs- und Kontrollbesuchs beim zuständigen Bundeszentralamt für Steuern zu kontrollieren.

### 9.3 Einführung der Elektronischen Lohnsteuerkarte

*Mit der zum 1. Januar 2012 beabsichtigten Umstellung von der Papierlohnsteuerkarte auf das elektronische Verfahren wird die Automatisierung in der Finanzverwaltung qualitativ wie quantitativ eine neue Stufe erreichen. Das Vorhaben wirft zahlreiche datenschutzrechtliche Fragen auf.*

Die beim Bundeszentralamt für Steuern (BZSt) eingerichtete Datenbank zur Steuer-Identifikationsnummer (Steuer-ID) wird derzeit um zusätzliche für den Lohnsteuerabzug benötigte Daten erweitert. Die gemäß § 39e EStG in der Datenbank gespeicherten **E**lektronischen **L**ohn**St**euer**A**bzugs**M**erkmale (ELStAM) beinhalten neben steuerlich relevanten Daten weitere, zum Teil sensible personenbezogene Daten etwa zu Religionszugehörigkeit, Familienstand oder Angehörigen (vgl. Kasten a zu Nr. 9.3). Zwar werden im Zusammenhang mit der Einführung der Elektronischen Lohnsteuerkarte keine neuen personenbezogenen Daten der Steuerpflichtigen erhoben, gleichwohl werden die bislang dezentral bei Meldebehörden und Finanzämtern gespeicherten Daten erstmalig in einer zentralen Datenbank erfasst. Die erweiterte Datenbank wird nach Ihrer Inbetriebnahme sensible Lohnsteuerdaten von mehr als 40 Millionen Arbeitnehmern enthalten. Auf die damit verbundenen Risiken habe ich bereits mehrfach hingewiesen (vgl. 22. TB Nr. 9.3).

Mit dem Jahressteuergesetz 2010 wurden in § 52b EStG ergänzende Regelungen zur Elektronischen Lohnsteuerkarte verabschiedet. Ich habe mich im Gesetzgebungsverfahren für eine Verbesserung der vorgesehenen Datenschutzvorgaben eingesetzt. Zu begrüßen ist, dass der Deutsche Bundestag meiner Empfehlung gefolgt ist, die betroffenen Arbeitnehmer rechtzeitig vor dem Starttermin des neuen Verfahrens durch die Finanzämter über die gebildeten ELStAM zu informieren (vgl. Bundestagsdrucksachen 17/3549 S. 29 und 17/3349 S. 44). Der ursprünglich vorgelegte Gesetzentwurf der Bundesregierung sah eine solche Regelung nicht vor. Die betroffenen Arbeitnehmer erhalten damit die Möglichkeit, die beim BZSt gebildeten ELStAM auf ihre Richtigkeit hin zu überprüfen und etwaige Fehler bei der Datenerfassung noch vor dem Abruf durch den Arbeitgeber zu korrigieren.

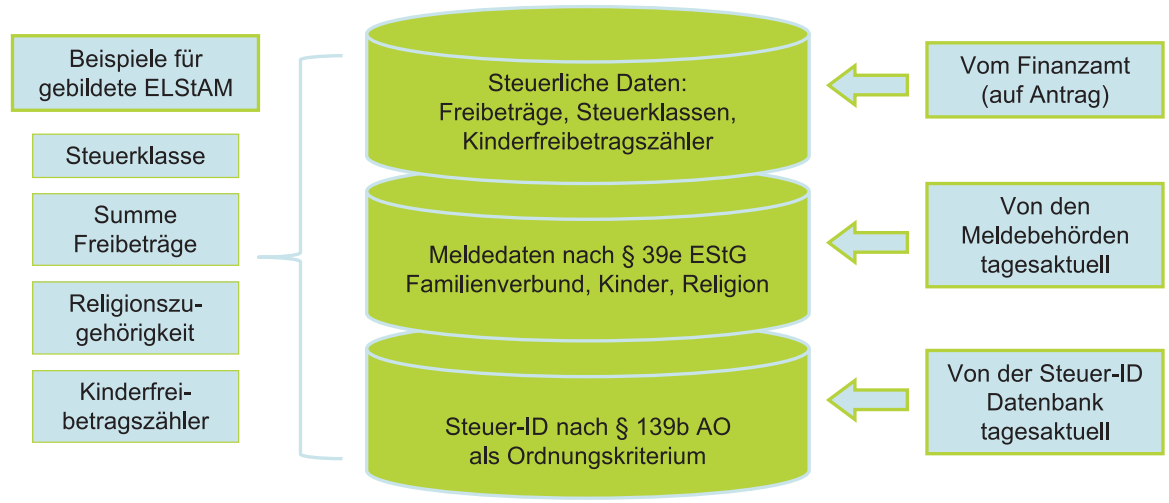
Die gespeicherten Datensätze sollen bundesweit ca. vier Millionen Arbeitgebern zum Abruf zur Verfügung stehen. Die für den Abruf erforderliche Authentisierung des Arbeitgebers über das ELSTER-Online Portal bewerte ich kritisch, da ELSTER-Online in erster Linie der elektronischen Übermittlung von Dokumenten der Steuerpflichtigen an die Finanzverwaltung dient (vgl. Nr. 3.6). Zweifel bestehen, ob es sich auch als Abrufportal für Arbeitgeber eignet, da ein Nachweis der Eigenschaft als Arbeitgeber und der Berechtigung zur Abfrage aufgrund der technischen Rahmenbedingungen bislang nicht hinreichend gewährleistet ist. Aufgrund der Sensibilität der Datensätze muss das Risiko eines unzulässigen Datenabrufs aber soweit wie möglich ausgeschlossen werden. Die Finanzverwaltung muss die dazu erforderlichen technisch-organisatorischen Maßnahmen treffen. Vor diesem Hintergrund ist zu begrüßen, dass Arbeitnehmerinnen und Arbeitnehmer aufgrund einer mit § 52b Absatz 8 EStG neu eingeführten Regelung die Bereitstellung der ELStAM über das zuständige Finanzamt allgemein sperren oder die Bereitstellung nur für bestimmte Arbeitgeber freigeben (Positivliste) bzw. ausschließen (Negativliste) lassen können.

Mit Blick auf die zum Aufbau der ELStAM-Datenbank durchgeführte Übermittlung der bislang bei den Meldebehörden als örtlichen Landesfinanzbehörden gespeicherten steuerlich relevanten Daten an das BZSt habe ich darauf hingewiesen, dass ein IT-verfahrensspezifisches Sicherheitskonzept für die Datenbank parallel zur Datenübermittlung zu entwickeln ist. Das Bundesministerium der Finanzen hat mir die Entwicklung eines verfahrensspezi-

fischen Sicherheitskonzeptes zugesagt, das ich nach Fertigstellung und Übersendung prüfen werde. Gemeinsam mit den Datenschutzbeauftragten der Länder werde ich mich weiterhin für einen besseren Schutz der in der zentralen Steuerdatenbank gespeicherten sensiblen Lohnsteuerdaten einsetzen (vgl. dazu auch die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 24. Juni 2010 – Kasten b zu Nr. 9.3).

Kasten a zu Nr. 9.3

**Inhalt der ELStAM Datenbank**




Kasten b zu Nr. 9.3

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Erweiterung der zentralen Steuerdatenbank um Elektronische Lohnsteuerabzugsmerkmale vom 24. Juni 2010**

**Erweiterung der Steuerdatenbank enthält große Risiken**

Bundesrat und Bundestag beraten in Kürze über die im Jahressteuergesetz 2010 vorgesehenen ergänzenden Regelungen zur Erweiterung der zentralen Steuerdatenbank. Die Datenbank soll um Elektronische Lohnsteuerabzugsmerkmale (ELStAM), wie z. B. sensible Angaben zu Religionszugehörigkeit und Familienangehörigen, ergänzt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, diese Regelungen kritisch daraufhin zu prüfen, ob sie datenschutzrechtlichen Belangen genügen und die Rechte der betroffenen Arbeitnehmer hinreichend wahren. Folgende Punkte müssen besondere Beachtung finden:

– *Vorherige Information der Arbeitnehmer*
Mit der Bildung der Elektronischen Lohnsteuerabzugsmerkmale ist die Ablösung der Papierlohnsteuerkarte verbunden. Um eine transparente Verfahrensumstellung zu gewährleisten, müssen die betroffenen Arbeitnehmer vor der erstmaligen Anwendung über die sie jeweils konkret betreffenden neuen Merkmale informiert werden. Dies ermöglicht den Arbeitnehmern, etwaige Fehler in der Datenerfassung beim Bundeszentralamt für Steuern vor dem Datenabruf durch den Arbeitgeber zu korrigieren.

– *Keine Speicherung auf Vorrat*
In der zentralen Datenbank sollen auch Datensätze zu Personen erfasst werden, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Speicherung von Datensätzen auf Vorrat ist verfassungsrechtlich höchst fragwürdig. Im Rahmen eines anlassbezogenen Vorgehens sollten Datensätze nur zu solchen Personen gespeichert werden, die tatsächlich lohnsteuerpflichtig sind.

– *Verhindern des unzulässigen Datenabrufs*
Die gespeicherten Datensätze werden bundesweit ca. vier Millionen Arbeitgebern zur Verfügung stehen. Ein Abruf der Elektronischen Lohnsteuerabzugsmerkmale soll nur möglich sein, wenn sich der Arbeitgeber oder ein von ihm beauftragter Dritter authentifiziert und seine Steuernummer mitteilt. Das vorgesehene Verfahren muss jedoch gewährleisten, dass nur befugte Arbeitgeber die Datensätze abrufen können. Ob dies tatsächlich erreicht wird, bleibt klärungsbedürftig. Ist ein unzulässiger Datenabruf nicht auszuschließen, sollte der Abruf generell nur unter Mitwirkung des betroffenen Arbeitnehmers möglich sein.

– *Kein Start ohne verfahrensspezifisches IT-Sicherheitskonzept*
Die erweiterte zentrale Datenbank wird sehr sensible steuerliche Daten von mehr als 40 Millionen Arbeitnehmern enthalten. Ein hoher Standard hinsichtlich der Datensicherheit muss daher spätestens mit Inbetriebnahme gewährleistet sein. Dies setzt voraus, dass ein umfassendes und vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorliegt. Die Erfahrung zeigt, dass die Entwicklung von IT-Sicherheitskonzepten für Datenbanken dieses Umfangs in zeitlicher Hinsicht einen längeren Vorlauf benötigt. Die notwendigen Arbeiten an einem IT-Sicherheitskonzept müssen unbedingt vor dem Aufbau der Datenbank abgeschlossen sein.

## 9.4 Schaffung eines Auskunftsrechts in der Abgabenordnung – eine „unendliche Geschichte“?

*Das verfassungsrechtlich gebotene Auskunftsrecht der Steuerpflichtigen gegenüber der Finanzverwaltung über die zu ihrer Person gespeicherten Daten ist grundsätzlich voraussetzungslos zu gewähren.*

Obwohl die seit langem erhobene Forderung der Datenschutzbeauftragten des Bundes und der Länder nach einer voraussetzungslosen Gewährleistung des Auskunftsrechts der Steuerpflichtigen (vgl. zuletzt 22. TB Nr. 9.5) durch einen Beschluss des Bundesverfassungsgerichts (BVerfG) vom 10. März 2008 (1 BvR 2388/0) gestärkt wurde, gewährt die Finanzverwaltung den Betroffenen weiterhin nur bei Darlegung eines „berechtigten Interesses“ Auskunft zu ihren gespeicherten Daten (vgl. Entschließung der 77. Datenschutzkonferenz, Kasten zu Nr. 9.4). Diese weitgehende Einschränkung des Auskunftsrechts steht in Widerspruch zum BDSG und den Landesdatenschutzgesetzen. Der auch gegenüber der Finanzverwaltung anwendbare § 19 BDSG räumt den Betroffenen grundsätzlich einen weitreichenden Anspruch auf Auskunft ein. Das Datenschutzrecht erkennt von vornherein ein Interesse des Einzelnen an der Auskunftserteilung an, da andererseits die verfassungsrechtlich gewährleisteten Rechte der Betroffenen unverhältnismäßig verkürzt würden. Die fortgesetzte und durch eine Dienstanweisung des Bundesministeriums der Finanzen (BMF) bekräftigte Verweigerung der auf Grund der Verfassung gebotenen Auskunftsrechte habe ich daher nach § 25 Absatz 1 BDSG förmlich beanstandet.

Das BMF hat daraufhin einen Diskussionsentwurf vorgelegt, mit dem ein gesetzlicher Auskunftsanspruch in der Abgabenordnung geschaffen werden soll. Danach sollen die Betroffenen bereits bei Antragstellung ihr „Informationsinteresse“ an der Auskunftserteilung erläutern und die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Eine solche Verpflichtung schränkt das Recht auf informationelle Selbstbestimmung der Betroffenen immer noch unverhältnismäßig ein und ist deswegen nicht akzeptabel. Eine Präzisierung des Auskunftsinteresses kann erst – und auch nur dann – bedeutsam werden, wenn es zur Abwägung mit einem Gegeninteresse der Finanzverwaltung kommt. In der Entscheidung des BVerfG vom 10. März 2008 heißt es dazu ausdrücklich, dass das „Auskunftsinteresse nur dann zurückgestellt werden [darf], wenn ein gegenläufiges Geheimhaltungsinteresse das Auskunftsinteresse im Rahmen einer Abwägung aller wesentlichen Umstände überwiegt“ (BVerfG, a. a. O., Rd. 103). Auch der Deutsche Bundestag hat in seiner Entschließung zu meinem 22. Tätigkeitsbericht vom 16. Dezember 2010 erneut gefordert, einen vorbehaltlosen Auskunftsanspruch zu gewährleisten (vgl. unter Nr. 15, Anlage 5).

Gegenüber dem BMF habe ich mich deshalb für die Schaffung einer gesetzlichen Regelung eingesetzt, die nicht hinter dem durch § 19 BDSG gewährleisteten und verfassungsrechtlich gebotenen Umfang zurückbleibt. Ich erwarte von der Bundesregierung und vom Deutschen Bundestag, dass sie endlich die datenschutzrechtlichen Defizite in der Abgabenordnung durch eine eindeutige Regelung beseitigen.

Kasten zu Nr. 9.4

**Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. März 2009 (Auszug)**

**Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten!**

…

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass das Bundesministerium der Finanzen die Verwaltungsanweisung vom 17. Dezember 2008 unverzüglich aufhebt. Die Finanzbehörden des Bundes und der Länder sind zu verpflichten, entsprechend der Rechtslage den Auskunftsanspruch zu erfüllen. Die Datenschutzbeauftragten des Bundes und der Länder appellieren zudem an den Bundesgesetzgeber, den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarzustellen, die dem § 19 BDSG entspricht.

## 9.5 Kirchensteuer auf Kapitalerträge: Soll meine Bank wissen, welcher Religion ich angehöre?

*Das künftige Verfahren des Kirchensteuerabzugs auf Kapitalerträge muss den besonderen datenschutzrechtlichen Anforderungen gerecht werden, die mit dem sensiblen Merkmal der Religionszugehörigkeit verbunden sind. Kreditinstitute sollten Kenntnis von der Religionszugehörigkeit ihrer Kunden nur mit deren Einwilligung erhalten.*

Seit 2009 wird die Kirchensteuer auf Kapitalerträge als Zuschlag zur Abgeltungssteuer erhoben. Die Steuerpflichtigen haben derzeit ein Wahlrecht, ob sie gegenüber den Kreditinstituten einen Antrag auf Kirchensteuerabzug stellen und ihnen zu diesem Zweck ihre Religionszugehörigkeit freiwillig mitteilen oder die Veranlagung durch das

Finanzamt durchführen lassen. Dieses nur für einen Übergangszeitraum vorgesehene Wahlverfahren soll nach dem Willen des Gesetzgebers durch ein Verfahren abgelöst werden, bei dem die auf Kapitalerträge anfallende Kirchensteuer grundsätzlich an der Quelle, d. h. bei den Kreditinstituten, erhoben wird. (vgl. hierzu 22. TB Nr. 9.2)

Dem gesetzlichen Auftrag aus § 51a Absatz 2e EStG folgend und in Vorbereitung der Einführung eines neuen Verfahrens hat das Bundesministerium der Finanzen (BMF) unter Beteiligung von Vertretern der Kirchensteuern erhebenden Religionsgemeinschaften und weiterer Sachverständiger das derzeitige Wahlverfahren evaluiert. Ich wurde hieran erst zu einem Zeitpunkt beteiligt, als die Evaluierung bereits weitgehend abgeschlossen war. Dies habe ich gegenüber dem BMF kritisiert, da datenschutzrechtliche Belange im Umgang mit dem besonders sensiblen personenbezogenen Merkmal Religionszugehörigkeit nicht hinreichend gewahrt wurden.

Kritisch bewertet hatte ich insbesondere, dass sich die Evaluierung auf ein System fokussiert hat, das es den zum Kirchensteuerabzug verpflichteten Kreditinstituten künftig ermöglichen soll, die Religionszugehörigkeit ihrer Kunden unmittelbar beim Bundeszentralamt für Steuern abzufragen. Zwar ist nach § 51a Absatz 2e EStG die Evaluierung mit dem Ziel durchzuführen, einen umfassenden verpflichtenden Quellensteuerabzug auf der Grundlage eines elektronischen Informationssystems zu ermöglichen. Dieser gesetzliche Auftrag entbindet jedoch nicht davon, alternative Modelle zur Erreichung dieses Zieles zu prüfen. Ich habe daher in enger Abstimmung mit den Landesbeauftragten für den Datenschutz eine Alternative vorgeschlagen, bei der die Kreditinstitute keine Kenntnis von der konkreten Religionszugehörigkeit ihrer Kunden erlangen. Dieses Modell beschränkt den Abruf im automatisierten Verfahren auf die Angabe des Prozentsatzes des abzuführenden Kirchensteuersatzes. Eine Clearingstelle würde die Zuordnung der abgeführten Kirchensteuer sowie deren Veranlagung und Weiterleitung durchführen. Trotz meiner späten Beteiligung an der Evaluierung konnte ich erreichen, dass mein Vorschlag Eingang in den Bericht fand, verbunden mit dem Auftrag der weiteren Prüfung (vgl. Bundestagsdrucksache 17/2865).

Das künftige Verfahren habe ich zwischenzeitlich mit Vertretern der zuständigen Arbeitsgruppe erörtert und dabei vor allem meine erheblichen Bedenken an den Vorschlägen des BMF deutlich gemacht. Die Kreditinstitute würden Kenntnis von der konkreten Religionszugehörigkeit von mehr als 90 Millionen Kontoinhabern erhalten, was zu erheblichen Missbrauchsrisiken führen und Begehrlichkeiten anderer Stellen wecken könnte. Auch habe ich Zweifel, inwieweit das beabsichtigte Verfahren mit dem Grundsatz der Datensparsamkeit vereinbar ist. Das von mir vorgeschlagene alternative Modell, bei dem die Kreditinstitute keine Kenntnis von der konkreten Religionszugehörigkeit ihrer Kunden erhalten, wurde von der Arbeitsgruppe jedoch nicht aufgegriffen.

Allerdings konnte ich erreichen, dass datenschutzrechtliche Belange bei der Ausgestaltung des künftigen Verfahrens besondere Berücksichtigung finden sollen: Um dem sensiblen Charakter der Religionszugehörigkeit gerecht zu werden, sollte die Übermittlung der entsprechenden Angaben an die Kreditinstitute nur mit Einwilligung der Kontoinhaber erfolgen. Zur Verringerung der Missbrauchsrisiken sollte den Kreditinstituten nicht die konkrete Religionszugehörigkeit, sondern allein eine entsprechend verschlüsselte Kennziffer übermittelt wird. Außerdem muss eine organisatorisch-technische Trennung des Verfahrens vom operativen Vor-Ort-Geschäft der Banken gewährleisten, dass beispielsweise der betreuende Bankbearbeiter keine Kenntnis von der Religionszugehörigkeit seiner Kunden erhält.

Ich werde die zum Redaktionsschluss noch nicht abgeschlossenen Überlegungen zur Einführung eines neuen Verfahrens weiterhin kritisch begleiten.

## 9.6 Prüfung einer Familienkasse

*Aus der Stellung der Familienkasse bei der Bundesagentur für Arbeit (BA) einerseits und der Wahrnehmung der Aufgaben einer Finanzbehörde andererseits ergeben sich datenschutzrechtliche Schwierigkeiten.*

Familienkassen sind Finanzbehörden, die für die Durchführung aller mit dem Kindergeld im Zusammenhang stehenden Leistungen zuständig sind. Sie werden von der BA als sog. Besondere Dienststellen getrennt von ihren übrigen Aufgaben geführt. Dieses Spannungsverhältnis zwischen den Aufgaben einer Finanzbehörde einerseits und der Zugehörigkeit zur BA andererseits führt zu datenschutzrechtlich kritischen Verflechtungen, die Gegenstand eines Kontroll- und Beratungsbesuchs waren. Problematisch sind insbesondere die wechselseitigen Zugriffsrechte auf Datensätze der Familienkasse bzw. der BA und der gemeinsame Versand von Postsendungen.

Bei der Ausgestaltung der Zugriffsrechte führte mein Kontrollbesuch zu dem als positiv zu bewertenden Ergebnis, dass Mitarbeiter der Familienkasse zwar auf das Vermittlungsprogramm „VerBIS“ der BA (vgl. hierzu 20. TB Nr. 16.2) zugreifen können, dieser Zugriff aber nur bei Vorliegen einer Einwilligung der Betroffenen erfolgt und auf die für die Bearbeitung von Kindergeldangelegenheiten erforderlichen Daten beschränkt ist.

Die Kontrolle offenbarte jedoch Defizite im Hinblick auf die gemeinsame Archivierung von Akten der Familienkasse und der örtlichen Agentur für Arbeit. Da dieser Missstand unmittelbar nach meinem Besuch beseitigt wurde, habe ich von einer Beanstandung abgesehen. Des Weiteren ergab meine Kontrolle, dass das Berechtigungskonzept für das von den Familienkassen eingesetzte IT-Verfahren KIWI (Kindergeld-Windows-Implementierung) den datenschutzrechtlichen Anforderungen an eine transparente Zuordnung von Aufgaben nicht ausreichend gerecht wird. Ich habe darauf hingewiesen, dass im Zusammenhang mit der derzeit parallel durchgeführten Erarbeitung eines neuen einheitlichen Benutzermanagement-Systems für alle Fachverfahren ein Berechtigungskonzept eingeführt werden sollte, das eine klare Zuordnung von Zugriffsbefugnissen zu einer bestimmten Aufgabe enthält. Dies wurde mir von der Familienkasse

zugesagt. Ich werde prüfen, inwieweit meinen Anregungen gefolgt wird.

### 9.7 Informationsaustausch in Steuersachen mit anderen Staaten

*Der internationale Informationsaustausch in Steuersachen hat in jüngerer Zeit an Bedeutung gewonnen. Datenschutzrechtliche Aspekte müssen dabei berücksichtigt werden.*

Als Folge der weltweiten Finanz- und Wirtschaftskrise soll die Zusammenarbeit in Steuersachen zwischen den Staaten verstärkt werden, insbesondere im Hinblick auf den Informationsaustausch unter den Steuerbehörden. Unter der Federführung der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) wurden in diesem Zusammenhang detaillierte Standards für den entsprechenden Informationsaustausch erarbeitet. Deutschland trifft derzeit mit Staaten mit wichtigen Finanzzentren bilaterale Vereinbarungen, die einen Informationsaustausch nach OECD-Standards ermöglichen sollen.

Im Rahmen meiner Beteiligung wirke ich darauf hin, dass bei den Verfahren zum zwischenstaatlichen Austausch von Steuerdaten datenschutzrechtliche Belange berücksichtigt werden. Dies gilt vor allem für einen automatischen Informationsaustausch, bei dem personenbezogene Daten periodisch ohne ein bestimmtes Ersuchen übermittelt werden, sowie den spontanen Informationsaustausch, bei dem ein Staat Kenntnisse, die für andere Staaten relevant sein könnten, unaufgefordert übermittelt. Die beiden letztgenannten Formen des Informationsaustausches stellen einen ungleich intensiveren Eingriff in das Recht auf informationelle Selbstbestimmung dar als die herkömmliche Datenübermittlung auf Ersuchen und bedürfen deshalb insbesondere der genauen Bestimmung ihres Zwecks und Umfangs.

### 9.8 Kontrolle des Kontenabrufverfahrens nach § 24c Kreditwesengesetz

*§ 24c Kreditwesengesetz – KWG – verpflichtet alle Kreditinstitute zur Führung einer Datei, aus der die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ohne Wissen der Kreditinstitute Kontostammdaten automatisiert abrufen kann. Im Frühjahr 2010 habe ich mir bei einer Kontrolle ein Bild von der Praxis des Kontenabrufs gemacht.*

Die Abrufe von Kontostammdaten durch die BaFin dienen der Erfüllung ihrer aufsichtlichen Aufgaben sowie der Auskunftserteilung auf Ersuchen (vgl. 19. TB Nr. 10.2; 20. TB Nr. 11.3.1). Die Zahl der fast ausschließlich von Strafverfolgungsbehörden gestellten Ersuchen hat sich von ca. 40 000 zu ca. 235 000 Konten im Jahre 2004 auf ca. 92 000 zu ca. 870 000 Konten im Jahre 2009 mehr als verdoppelt und bezogen auf die genannten Kontenzahlen um das rund 3,7-fache erhöht.

Seit März 2008 bedient sich die BaFin der technischen Komponenten des Kontenabrufs des Zentrums für Informationsverarbeitung und Informationstechnik (ZIVIT) als Auftragsdatenverarbeiter. Daher hätte bereits damals ein entsprechender Vertrag zwischen BaFin und ZIVIT geschlossen werden müssen. Aufgrund von Umsetzungsproblemen im ZIVIT erfolgte dessen Unterzeichnung erst nach meiner Kontrolle. Dies bot mir Gelegenheit zu Empfehlungen zum Vertragsentwurf, denen die Vertragsparteien folgten.

Das gilt auch für eine mittlerweile implementierte automatische Löschroutine zur Gewährleistung der fristgerechten Löschung der in § 24c Absatz 4 KWG erwähnten Protokolldaten.

Zum Zeitpunkt der Kontrolle fehlte es wegen der erwähnten Umsetzungsprobleme im ZIVIT an der Vereinbarung eines IT-Sicherheitskonzepts. Auch dieser Kritikpunkt wurde unter Berücksichtigung meiner Anregungen ausgeräumt.

Die BaFin hat meine Kontrolle mit hoher Kooperationsbereitschaft begleitet. Sie hat meine datenschutzbezogenen Anregungen mittlerweile vollständig aufgegriffen. Hierzu zählen neben kleineren Justierungen in der Ablauforganisation auch die erforderlichen Verbesserungen im Bereich der Datensicherheit.

## 10 Wirtschaft und Verkehr

### 10.1 Binding Corporate Rules

*Das Verfahren zur Annahme von Unternehmensregelungen für die Übermittlung von Daten aus der EU in Drittstaaten (Binding Corporate Rules, BCR) wurde deutlich beschleunigt. Ich konnte im Berichtszeitraum die Prüfung der BCR der Deutschen Post AG nach dieser Vorgehensweise erfolgreich abschließen.*

Die europäische Datenschutzrichtlinie sieht vor, dass die Übermittlung personenbezogener Daten in Drittstaaten ohne angemessenes Datenschutzniveau ausnahmsweise genehmigt werden kann (Artikel 26 der europäischen Datenschutzrichtlinie 95/46/EG). Unternehmen müssen hierzu ausreichende Datenschutzgarantien abgeben, u. a. durch BCR. Die Art.-29-Gruppe setzte im Berichtszeitraum ihre Bemühungen fort, das BCR-Verfahren zu vereinfachen und zu vereinheitlichen. Zu einer erheblichen Beschleunigung trug dabei das im Jahr 2008 zwischen den Datenschutzaufsichtsbehörden mehrerer Mitgliedstaaten vereinbarte „Verfahren der gegenseitigen Anerkennung“ bei. Danach wird ein positives Prüfungsergebnis der Datenschutzaufsichtsbehörde zu den BCR eines Unternehmens im federführenden Mitgliedsstaat von den Behörden der anderen Mitgliedstaaten als ausreichende Grundlage angesehen, den BCR ihrerseits zuzustimmen (vgl. 22. TB Nr. 13.2.3). Dem Verfahren haben sich inzwischen 19 europäische Datenschutzaufsichtsbehörden angeschlossen. Überarbeitet wurde darüber hinaus die Zusammenstellung häufig gestellter Fragen, mit der den Unternehmen vermittelt werden soll, welche Anforderungen die europäischen Datenschutzaufsichtsbehörden an BCR stellen (WP 155 Rev. 4 vom 8. April 2009).

Im Jahr 2007 hatte die Deutsche Post AG – ein global agierender Konzern, der ständig Kunden- und Beschäftig-

tendaten über alle Grenzen hinweg austauscht – mich gebeten, federführend das europaweite Verfahren zur Prüfung verbindlicher Unternehmensregelungen nach den Vorgaben der Artikel-29-Gruppe durchzuführen. Da während des Abstimmungsprozesses das Verfahren der gegenseitigen Anerkennung etabliert wurde, konnte auch die Prüfung der BCR der Deutschen Post AG im Dezember 2010 nach dieser Vorgehensweise auf europäischer Ebene abgeschlossen werden. Ebenso habe ich die nach mehrheitlicher Auffassung der Aufsichtsbehörden erforderliche einmalige Genehmigung der Datenübermittlung nach Maßgabe der vorgelegten BCR gemäß § 4c Absatz 2 BDSG erteilt. Mit der Einführung der verbindlichen Unternehmensregelungen wird die Deutsche Post AG nunmehr ein Netz von Datenschutzbeauftragten im gesamten Konzern aufbauen.

### 10.2 Kontrolle des Verfahrens zur „Kfz-Umweltprämie“ beim Bundesamt für Ausfuhrkontrolle

*Bei dem unter großem Zeitdruck eingeführten Verfahren zur Bearbeitung von Anträgen zur Gewährung einer „Kfz-Umweltprämie“ gab es vielfältige Datenschutzprobleme, die mich veranlassten, gegenüber dem Bundesministerium für Wirtschaft und Technologie zwei formelle Beanstandungen auszusprechen. Meinen Forderungen und Empfehlungen wurde Rechnung getragen.*

Anfang 2009 konnte man den Eindruck gewinnen, ganz Deutschland verschrottet seine Gebrauchtwagen und erwirbt neue Fahrzeuge. Ganz Deutschland? Nein, nur diejenigen, die sich die im Volksmund als „Abwrackprämie“ bezeichnete Leistung sichern wollten. Die Prämie von 2 500 Euro wurde vom Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) bei Vorliegen bestimmter Voraussetzungen ausgezahlt.

Zunächst hatte das BAFA nur ein einstufiges Verfahren eingerichtet, wonach der Antragsteller einen Vordruck aus dem Internet herunterladen und diesen ausgefüllt zusammen mit diversen Unterlagen an das BAFA senden musste. Dabei mussten zunächst das Altfahrzeug verschrottet und das neue Fahrzeug zugelassen sein, bevor der Antrag gestellt werden konnte. Käufer von Fahrzeugen mit langen Lieferzeiten waren in diesem „Windhundverfahren“ benachteiligt. Um auch diesem Personenkreis die Inanspruchnahme der Prämie zu ermöglichen, wurde das Verfahren ab dem 30. März 2009 durch ein zweistufiges Online-Reservierungsverfahren abgelöst, mit dem die Umweltprämie durch Vorlage eines gültigen Kaufvertrags reserviert werden konnte.

In meiner Dienststelle ging in den ersten Stunden nach dem Start des Online-Verfahrens eine Vielzahl von Beschwerden ein. So wurde das von dem BAFA online gestellte Antragsformular, in dem eine Vielzahl personenbezogener Daten anzugeben waren, nur über eine nicht verschlüsselte Internetverbindung übertragen. Hinzu kam, dass die Website wegen der enormen Resonanz (in den ersten Tagen wurden bereits über 650 000 Anträge gestellt) schnell überlastet war und auf das Online-Formular nicht mehr zugegriffen werden konnte. Daraufhin nahm das BAFA ein technisches Duplikat der Online-Antragsumgebung auf zusätzlichen Computersystemen in Betrieb. Dies führte jedoch zu einem weiteren Problem: Automatisch generierte Eingangsbestätigungen, die neben einer fortlaufenden Registriernummer auch alle vom Antragsteller angegebenen Daten enthielten, wurden an die falschen Adressaten gesandt. Die Duplizierung hatte zu einer doppelten Vergabe von Registriernummern geführt.

Ich habe umgehend beim BAFA darauf hingewirkt, diese Probleme unverzüglich abzustellen. Die Fehlerquelle, die für die doppelte Vergabe von Registriernummern verantwortlich war, wurde schnell gefunden und beseitigt; betroffen waren etwa 200 Antragsteller. Leider war das BAFA nicht in der Lage, die Internetverbindung kurzfristig sicher zu gestalten. Erst gut zwei Wochen später konnten die notwendigen Komponenten für eine verschlüsselte Übertragung der Formulardaten installiert werden. Dieser Umstand hat mich veranlasst, zwei Beanstandungen gegenüber dem Bundesministerium für Wirtschaft und Technologie auszusprechen.

Letztlich wurden rund 2 Millionen Anträge bearbeitet. Ich habe mir deshalb auch einen Überblick über die Datenerhebung und -verarbeitung bei Beantragung und Gewährung der Umweltprämie beim BAFA-Standort in Eschborn verschafft.

Dabei habe ich berücksichtigt, dass dieses aufwändige Massenverfahren aufgrund der politischen Vorgaben innerhalb weniger Arbeitstage vollständig umzusetzen war und sich das BAFA deshalb diverser externer Dienstleister bedienen musste. Mit allen Auftragnehmern hat das BAFA entsprechende Verträge geschlossen. Die datenschutzrechtlichen Vorgaben des § 11 BDSG zur Auftragsdatenverarbeitung waren im Großen und Ganzen eingehalten (vgl. zu § 11 BDSG auch Nr. 2.4). Ich habe empfohlen, bei künftigen Aufträgen z. B. Vor-Ort-Kontrollen des behördlichen Datenschutzbeauftragten bei den Auftragnehmern durchzuführen.

Meine Empfehlung, die im Zuge der Antragstellung bei den Dienstleistern entstandenen redundanten Datenbestände zu löschen, wurde inzwischen umgesetzt. Ich habe dem BAFA nahegelegt, für vergleichbare künftige Verfahren die Löschung von personenbezogenen Daten unmittelbar nach Wegfall der Erforderlichkeit sicherzustellen.

Im Zuge der Antragsbearbeitung musste das BAFA sein Stammpersonal intern umsetzen und auch zusätzlich Zeitarbeitskräfte beschäftigen; insgesamt waren bis zu 250 Personen mit der Bearbeitung von Anträgen betraut. Auch wurde eine Telefon-Hotline eingerichtet, um allgemeine Fragen schnellstmöglich zu beantworten. Die Mitarbeiter dieser Hotline hatten keinen Zugriff auf die Datenbank; auch hatte das BAFA dafür Sorge getragen, dass die Anträge bearbeitenden Mitarbeiter nur ihren Aufgaben entsprechenden Zugriff auf die Datenbank hatten.

Die von meinen Mitarbeitern vor Ort festgestellten Mängel der Systemadministration wurden behoben. So wurden die Vorgaben zur Gestaltung des Passwortes überarbeitet und verändert. Auch wurde meiner Empfehlung

gefolgt, die Benutzerverwaltung, das Passwortmanagement und das Rollenkonzept in Bezug auf die Administratorrechte so zu überarbeiten, dass der behördliche Datenschutzbeauftragte in angemessener Zeit Kontrollen durchführen und die Benutzerrechte effizient kontrollieren kann.

## 10.3 Forschungsprojekte beim Max-Rubner-Institut

*Das Max-Rubner-Institut führt bundesweite Studien zur Ernährung und zum gesundheitlichen Verbraucherschutz durch und erhebt dafür eine Vielzahl personenbezogener Daten.*

Im Max-Rubner-Institut (MRI), einer Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV), sind seit dem 1. Januar 2008 alle Bundesforschungsanstalten im Bereich Lebensmittel und Ernährung zusammengefasst. Forschungsschwerpunkt ist der gesundheitliche Verbraucherschutz im Ernährungsbereich. Die Bundesforschungsinstitute haben die Aufgabe, unabhängige und belastbare wissenschaftliche Grundlagen als Entscheidungshilfen für die Politik bereitzustellen und Verbraucherinnen und Verbrauchern wichtige Erkenntnisse zu vermitteln.

Im Berichtszeitraum habe ich das MRI im Hinblick auf die Nationale Verzehrsstudie (NVS) II und das Nationale Ernährungsmonitoring (NEMONIT) kontrolliert.

Die NVS II hat zum Ziel, für Deutschland repräsentative Daten zum aktuellen und üblichen Verzehr von Lebensmitteln aufzuzeigen. Mit dem Management für die Erhebung, Speicherung und Nutzung der Kontakt- sowie der Studiendaten der Teilnehmer wurde die Firma TNS Healthcare betraut, ein Marktforschungsinstitut im Gesundheitsbereich. Aus datenschutzrechtlicher Sicht ist weder das Datenmanagement der TNS Healthcare noch des MRI zu beanstanden.

Mit NEMONIT soll die Ernährung der deutschen Bevölkerung langfristig erfasst werden, um aktuelle Daten für ernährungspolitische Maßnahmen und für die Ernährungsforschung zu liefern. Wie bei der NVS II ist das MRI für die Planung und Koordination der Studie sowie die Aufbereitung und Auswertungen der Rohdaten zuständig. Die Durchführung der Felderhebungen wurde für die Dauer von drei Jahren an das Marktforschungsinstitut Produkt + Markt in Wallenhorst vergeben. Die Erhebung, Speicherung und Nutzung der Daten bei NEMONIT orientiert sich an der NVS II und verwendet auch einen Teil der hierfür erhobenen Daten.

Anfängliche Probleme mit dem Vertrag zwischen dem MRI und Produkt + Markt über die Verarbeitung personenbezogener Daten im Auftrag nach § 11 BDSG konnten gelöst werden (vgl. zu § 11 BDSG auch Nr. 2.4). Ebenso hat das MRI fehlerhafte Formulierungen im Dateiverzeichnis sowie dem Erläuterungsanschreiben zu NEMONIT korrigiert.

Die Rekrutierung der Teilnehmer aus dem Kreis der bereits an der NVS II Beteiligten führte dazu, dass 148 der Befragten keine schriftliche Einwilligung in die Datenerhebung, -speicherung und Nutzung im Rahmen dieser Studie abgegeben haben. Aus datenschutzrechtlicher Sicht bedarf die Einwilligung der Schriftform, soweit nicht aufgrund besonderer Umstände eine andere Form angemessen ist. Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand dann vor, wenn durch die Schriftform der Forschungszweck erheblich beeinträchtigt würde. Müsste das MRI mangels Schriftform auf die bisher erhobenen Daten der Teilnehmer verzichten, würde das Ergebnis der Studie in Teilen verzerrt und seine Aussagekraft stark reduziert werden. Folglich würde der Forschungszweck erheblich beeinträchtigt werden. Daher habe ich im vorliegenden Fall davon abgesehen, die nachträgliche Einholung schriftlicher Einwilligungserklärungen zu verlangen. Allerdings rege ich an, bei neuen Teilnehmerinnen und Teilnehmern und bei vergleichbaren zukünftigen Erhebungen generell schriftliche Einwilligungen zu verwenden.

Ferner habe ich geprüft, ob das MRI die gespeicherten Daten entsprechend den gesetzlichen Vorgaben löscht: Das MRI speichert nämlich auch die personenbezogenen Daten der Teilnehmer aus der NVS II, die eine Teilnahme an einer weiteren Befragung abgelehnt haben. Verwendet das MRI diese Daten zur erneuten Kontaktaufnahme, kommt dies einer Speicherung, Veränderung oder Nutzung für andere Zwecke gleich, die gemäß § 14 Absatz 2 Nr. 9 BDSG nur zulässig ist, wenn die im Zusammenhang mit dem Forschungsvorhaben stehenden Interessen überwiegen und nicht anders erreicht werden können. Auch hier konnte das MRI nachvollziehbar den Vorrang des wissenschaftlichen Interesses darlegen. Aus datenschutzrechtlicher Sicht ist damit eine Speicherung der Daten von Teilnahmeverweigerern – allerdings nur bis zu ihrer erneuten Ansprache – nicht zu beanstanden.

## 10.4 Quo vadis Düsseldorfer Kreis?

*Der „Düsseldorfer Kreis“ hat sich als Koordinierungsgremium der Aufsichtsbehörden und als Ansprechpartner der Wirtschaft fest etabliert. Er sollte auch nach der Umsetzung des EuGH-Urteils zur Unabhängigkeit der Aufsichtsbehörden als anerkanntes Markenzeichen erhalten bleiben.*

Der Düsseldorfer Kreis (DK), in dem die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich unter meiner Mitwirkung seit langem zusammenarbeiten, ist für die Koordination der Datenschutzaufsicht in Deutschland von zentraler Bedeutung. Für eine wirksame und überzeugende Datenschutzaufsicht ist ein zügiger Erfahrungs- und Informationsaustausch zwischen den Aufsichtsbehörden mit der Möglichkeit zur Erörterung rechtlicher Fragestellungen unerlässlich.

Die fortschreitende Globalisierung des Wirtschaftsverkehrs und die grenz- und länderübergreifenden Strukturen des Internets haben den Abstimmungsbedarf zwischen den Aufsichtsbehörden deutlich erhöht. Immer häufiger müssen sich diese mit Konstellationen befassen, die die Zuständigkeit mehrerer Aufsichtsbehörden berühren. Dies betrifft namentlich die Kontrolle deutschlandweit agieren-

der Unternehmen, die ihren Unternehmenssitz zudem häufig im Ausland haben. Hier muss nicht nur im Interesse eines effizienten Datenschutzes mit einer Stimme gesprochen werden, der DK übernimmt in diesen Fällen zugleich die wichtige Funktion eines vertrauenswürdigen Ansprechpartners für die Wirtschaft, der auch im Interesse der Daten verarbeitenden Stellen Rechtssicherheit schafft. Zu diesem Zweck hat der DK fachspezifische Arbeitsgruppen eingerichtet, die datenschutzrechtliche Fragen teilweise im direkten Kontakt mit der Wirtschaft erörtern.

So konnte der Düsseldorfer Kreis gegenüber den Internetdiensten Facebook (vgl. Nr. 4.5) und Google Street View (vgl. Nr. 4.1.1) eine einheitliche Rechtsposition entwickeln und hierdurch ein gemeinsames Vorgehen aller Aufsichtsbehörden sicherstellen. Hierzu wurden dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit die Koordination und Federführung der Gespräche mit den Unternehmen übertragen.

Darüber hinaus hat der DK auch im Berichtszeitraum zahlreiche Beschlüsse gefasst und unter anderem zu der Zulässigkeit der Anforderung von Bonitätsauskünften gegenüber Mietinteressenten, zu der Erstellung von Nutzungsprofilen durch Internetseiten-Betreiber und zu den datenschutzrechtlichen Voraussetzungen im Umgang mit Cookies nach Maßgabe der überarbeiteten Datenschutzrichtlinie für elektronische Kommunikationsdienste Stellung genommen. In einem weiteren Beschluss hat sich der DK mit der Formulierung von Mindestkriterien befasst, die das Daten exportierende Unternehmen zu beachten hat, bevor es personenbezogene Daten im Rahmen des Safe Harbor-Abkommens (vgl. Nr. 13.4) an ein US-Unternehmen übermittelt. (Alle Beschlüsse des Düsseldorfer Kreises im Berichtszeitraum: vgl. Kasten zu Nr. 10.4).

Die im Zuge des EuGH-Urteils zur Unabhängigkeit der Aufsichtsbehörden im nicht-öffentlichen Bereich fortschreitende Zusammenlegung der Aufsichtsbehörden mit den Landesdatenschutzbeauftragten (vgl. Nr. 2.1) wird auch Auswirkungen auf den DK und seine Arbeitsgruppen haben. Unabhängig davon, ob er weiterhin eigenständig bestehen bleibt oder als Arbeitskreis in die Konferenz der Datenschutzbeauftragten integriert wird – was ich begrüßen würde – sollte aber der Name „Düsseldorfer Kreis“ als in der Wirtschaft anerkanntes Markenzeichen zur Klärung von Sachfragen und rechtlichen Bewertungen erhalten bleiben.

Kasten zu Nr. 10.4

**Beschlüsse des Düsseldorfer Kreises in den Jahren 2009/2010:**

- Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste: Datenschutzrechtliche Voraussetzungen beim Umgang mit Cookies
- Mindestanforderungen an die Fachkunde und Unabhängigkeit der Beauftragten für den Datenschutz nach § 4f Absatz 2 und 3 BDSG
- Wirksamer Schutz Minderjähriger in sozialen Netzwerken
- Datenschutz im Verein: Umgang mit Gruppenversicherungsverträgen
- Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe-Habor-Abkommen durch das Daten exportierende Unternehmen
- Novellierung des BDSG bei der Datenverwendung für Werbezwecke
- Zulässigkeit der Internetveröffentlichung sportgerichtlicher Entscheidungen
- Voraussetzungen der Erstellung von Nutzungsprofilen durch Webseitenbetreiber
- Einholung von Bonitätsauskünften über Mietinteressenten
- Übermittlung von Passagierdaten an britische Behörden
- Telemarketing bei nichtstaatlichen Organisationen (NGO)
- Mitarbeiter-Screening in international tätigen Unternehmen

abrufbar über meine Website www.datenschutz.bund.de

## 10.5 Scoring: Noch viele Fragen offen

*§ 28b BDSG schafft erstmals eine ausdrückliche Rechtsgrundlage für die Durchführung von Scoringverfahren im BDSG. Ob die Regelung tatsächlich die versprochene Transparenz und Rechtssicherheit schafft, wird sich erst zeigen müssen. Derzeit sind noch viele Fragen offen.*

Mit dem am 1. April 2010 in Kraft getreten § 28b BDSG hat der Gesetzgeber eine Rechtsgrundlage geschaffen, die die Voraussetzungen für die Durchführung solcher Scoringverfahren festlegt, deren Ergebnisse für Entscheidungen über Vertragsverhältnisse verwendet werden. Scoringverfahren dienen im Wirtschaftsverkehr dazu, die Kreditwürdigkeit von Personen und die damit verbundenen Chancen und Risiken für die Vertragspartner einzuschätzen. Zu diesem Zweck werden im Vorfeld der Entscheidung über die Begründung, Durchführung oder Beendigung von Vertragsverhältnissen aus den über die Person vorhandenen Daten Scorewerte (Wahrscheinlichkeitswerte) errechnet, die eine möglichst genaue Aussage über die statistische Wahrscheinlichkeit treffen sollen, mit der der Schuldner seine vertragliche Verpflichtung erfüllen wird.

In der Vergangenheit war es den Datenschutzbehörden kaum möglich, Einblicke in das Verfahren zur Bildung der Scorewerte und die für die Ermittlung der Scorewerte verwendeten Daten zu erlangen. § 28b BDSG legt nunmehr Art und Umfang der zulässigen Datengrundlage fest. So müssen im Fall der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunftei die Voraussetzungen für eine zulässige Übermittlung der genutzten Daten nach § 29 BDSG, in allen anderen Fällen die Voraussetzungen einer

zulässigen Nutzung nach § 28 BDSG vorliegen (§ 28b Nr. 2). Zudem enthält die Vorschrift gewisse Einschränkungen bei der Verwendung von Anschriftendaten, nämlich dass die Beurteilung der Kreditwürdigkeit nicht ausschließlich anhand der Wohnanschrift ermittelt werden darf und die Betroffenen in jedem Fall bei der Nutzung von Anschriftendaten noch vor Berechnung des Scorewerts zu unterrichten sind (§ 28b Nr. 3 und 4). Und schließlich muss das Scoreverfahren wissenschaftlichen Ansprüchen genügen (§ 28b Nr. 1).

Auf das Verlangen der Datenschutzbehörden hin haben mittlerweile zwei große Auskunfteien Gutachten über diesen so genannten Wissenschaftlichkeitsnachweis vorgelegt.

Welche konkreten Anforderungen an den Wissenschaftlichkeitsnachweis zu stellen sind, haben die Datenschutzbehörden noch nicht abschließend beurteilt. Große Schwierigkeiten bereitet insbesondere die Frage, welche Aussagekraft die genutzten Daten unter Beachtung wissenschaftlicher Ansprüche haben müssen, damit sie tatsächlich, wie vom Gesetz gefordert, für die Berechnung des Wahrscheinlichkeitswertes „erheblich“ sind.

Weiterhin zwischen den Auskunfteien und den Datenschutzbehörden umstritten ist die Frage, inwiefern Angaben über Alter und Geschlecht in Scorewerte einfließen dürfen. Die Verwendung dieser Daten verstößt möglicherweise gegen das Allgemeine Gleichbehandlungsgesetz (AGG), das Benachteiligungen unter anderem aus Gründen des Geschlechts oder des Alters grundsätzlich für unzulässig erklärt. Ich habe mich in dieser Angelegenheit an das Bundesministerium der Justiz (BMJ) gewandt und um eine rechtliche Einschätzung gebeten. In seiner Stellungnahme hat das BMJ u. a. auf § 20 Absatz 1 Satz 1 AGG verwiesen, demzufolge für die Datengruppen des Alters und des Geschlechts Ausnahmen von dem Benachteiligungsverbot zulässig sein können, wenn ein sachlicher Grund für die Ungleichbehandlung vorliegt. Ob es tatsächlich, wie von den Auskunfteien vorgetragen, statistische Unterschiede im Zahlungsverhalten von Männern und Frauen sowie verschiedener Altersgruppen gibt, die einen sachlichen Grund für eine Ungleichbehandlung nach dem AGG darstellen können, wird weiter zu erörtern sein.

Auf die diskriminierende Wirkung der Verwendung von Adressdaten bei der Berechnung von Scorewerten bin ich bereits in meinem letzten Tätigkeitsbericht eingegangen (vgl. 22. TB Nr. 3.4.4). Das in § 28b Nr. 3 BDSG nunmehr vorgesehene Verbot der ausschließlichen Nutzung von Anschriften zum Zwecke der Berechnung von Wahrscheinlichkeitswerten reicht nicht aus und läuft in der Praxis häufig leer, da die Berechnung der Scorewerte in den seltensten Fällen allein anhand von Anschriftendaten erfolgt. Hier sehe ich noch Verbesserungsbedarf.

### 10.6 Schufa-Klausel: Totgesagte leben länger

*Mit der Schaffung des § 28a Absatz 2 BDSG hat der Gesetzgeber für bestimmte Bankgeschäfte die bisherige Einwilligungslösung („SCHUFA-Klausel“) durch eine gesetzliche Grundlage ersetzt. Dennoch wird die „SCHUFA-Klausel“ in der Bankenpraxis weiterhin verwendet.*

Mit dem durch die BDSG-Novelle I im April 2010 neu eingefügten § 28a BDSG (vgl. Kasten zu Nr. 10.6) hat der Gesetzgeber einen speziellen Erlaubnistatbestand zur Übermittlung von Daten an Auskunfteien geschaffen. Während § 28a Absatz 1 die Einmeldung von Daten über Forderungen (Negativdaten) regelt, ist es Kreditinstituten

Kasten zu Nr. 10.6

**§ 28a Datenübermittlung an Auskunfteien**

(1) Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit (...)

(2)Zur zukünftigen Übermittlung nach § 29 Absatz 2 dürfen Kreditinstitute personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft nach § 1 Absatz 1 Satz 2 Nr. 2, 8 oder Nr. 9 des Kreditwesengesetzes an Auskunfteien übermitteln, es sei sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt. Der Betroffene ist vor Abschluss des Vertrages hierüber zu unterrichten. Satz 1 gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben. Zur zukünftigen Übermittlung nach § 29 Absatz 2 ist die Übermittlung von Daten über Verhaltensweisen des Betroffenen, die im Rahmen eines vorvertraglichen Vertrauensverhältnisses der Herstellung von Markttransparenz dienen, an Auskunfteien auch mit Einwilligung des Betroffenen unzulässig.

**Auszug aus der Gesetzesbegründung, Bundestagsdrucksache 16/10529, S. 14 f.**

§ 28a Absatz 2 Satz 1 ist ein spezieller Erlaubnistatbestand für bestimmte Übermittlungen personenbezogener Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertrages im Rahmen eines Bankgeschäfts im Sinne des § 1 Absatz 1 Satz 2 Nr. 2 (Kreditgeschäft), Nr. 8 (Garantiegeschäft) oder Nr. 9 (Girogeschäft) KWG. Diese Datenübermittlungen werden mangels spezieller Rechtsgrundlage derzeit auf eine Einwilligung des Betroffenen nach § 4 BDSG gestützt. Dies ist insofern problematisch, als in der Praxis eine natürliche Person einen Bankkredit regelmäßig nicht mehr ohne eine von der Bank angeforderte Bonitätsauskunft einer Auskunftei erhält, wobei diese mit einer Einwilligungserklärung des Betroffenen in die Übermittlung bestimmter personenbezogener Daten an diese Auskunftei verbunden wird. Mangels zumutbaren Alternativverhaltens kann es daher zweifelhaft sein, ob die vom Betroffenen erteilte Einwilligung noch als freiwillig anzusehen ist. An die Stelle der Einwilligungserklärung tritt der neue Erlaubnistatbestand in Absatz 2 (...)

bei Vorliegen der Voraussetzungen des § 28a Absatz 2 auch erlaubt, personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung bestimmter Bankgeschäfte an die Auskunfteien zu melden. Bislang wurde die Übermittlung dieser so genannten Positivdaten von den Kreditinstituten an die Auskunfteien auf eine Einwilligung der Betroffenen nach § 4 BDSG gestützt. Wer ein Girokonto eröffnen oder einen Bankkredit haben wollte, wurde stets aufgefordert, seine Einwilligung zur Übermittlung der Daten an Auskunfteien zu erteilen (SCHUFA-Klausel).

An der Freiwilligkeit der bisherigen SCHUFA-Einwilligung haben die Datenschutzaufsichtsbehörden allerdings schon seit längerer Zeit erhebliche Zweifel geäußert. Wollen die Bankkunden nicht auf den Kredit oder den Abschluss eines Girovertrags verzichten, bleibt ihnen nämlich meist gar nichts anderes übrig, als die SCHUFA-Klausel zu unterschreiben. Die Freiwilligkeit der Entscheidung ist nach § 4a BDSG allerdings Wirksamkeitsvoraussetzung einer Einwilligung. Der Gesetzgeber hat aus diesem Grund mit § 28a Absatz 2 BDSG einen speziellen Erlaubnistatbestand für die Übermittlung vertragsbezogener Bankdaten des Kunden an Auskunfteien eingeführt, der nach dem gesetzgeberischen Willen an die Stelle der Einwilligungserklärung treten sollte.

Trotz dieser klaren Vorgaben wird von der SCHUFA-Klausel in der Bankenpraxis gleichwohl noch immer Gebrauch gemacht. Die Banken weisen unter anderem darauf hin, § 1 Absatz 1 Satz 2 Nr. 9 Kreditwesengesetz (KWG), auf welchen § 28a Absatz 2 Bezug nimmt, umfasse mittlerweile aufgrund einer Änderung seines Wortlautes nicht mehr das Girogeschäft, so dass es zumindest für Girokontoverträge weiterhin einer Einwilligungserklärung des Kunden bedürfe. Der Gesetzgeber sollte hier für Klarheit sorgen und § 28a Absatz 2 BDSG die von ihm intendierte Geltungskraft verschaffen.

## 10.7 Datenschutz in der Versicherungswirtschaft

*Die Verbesserung des Datenschutzes bei Versicherungsunternehmen kommt nur langsam voran. Eine neugefasste Einwilligungs- und Schweigepflichtentbindungserklärung soll aber endlich im Frühjahr 2011 vorliegen. Auch wird dann hoffentlich die überfällige datenschutzgerechte Umgestaltung des Hinweis- und Informationssystems (HIS) abgeschlossen sein. Für die Verarbeitung von Gesundheitsdaten muss eine zusätzliche gesetzliche Regelung geschaffen werden.*

### Einwilligungs- und Schweigepflichtentbindungserklärung

Über die Notwendigkeit, die von der Versicherungswirtschaft verwendete Einwilligungs- und Schweigepflichtentbindungserklärung zu überarbeiten, habe ich bereits mehrfach berichtet (vgl. zuletzt 22. TB Nr. 3.4.7). Meine damalige Annahme, die Überarbeitung würde bald abgeschlossen, hat sich leider nicht bestätigt. Die Beratungen der Datenschutzaufsichtsbehörden mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) kamen nicht richtig voran. Wegen der Dringlichkeit des Themas hat die AG Versicherungswirtschaft des Düsseldorfer Kreises deshalb einen eigenen Entwurf für eine neue Einwilligungsklausel erarbeitet und im März 2010 in die Verhandlungen mit dem GDV eingebracht. Nach dem Stand der Verhandlungen kann aber wohl im Frühjahr 2011 mit einem Konsens über den endgültigen Wortlaut der Einwilligungsklausel gerechnet werden.

Im Anschluss daran sollen auch wieder die Gespräche über eine vom GDV überarbeitete Version eines Code of Conduct (vgl. 22. TB Nr. 3.4.7) aufgenommen werden, die zunächst ausgesetzt worden sind.

### Hinweis- und Informationssystem (HIS)

Die datenschutzrechtlichen Bedenken gegen das Hinweis- und Informationssystem (HIS) der Versicherungswirtschaft, das der Risikoprüfung und Aufdeckung bzw. Verhinderung von Versicherungsbetrug dient, habe ich ebenfalls schon mehrfach thematisiert (vgl. zuletzt 22. TB Nr. 4.4.7). Der GDV hat zwar eine Neukonzeption vorgestellt, die eine Weiterführung von HIS als Auskunftei auf Grundlage von § 29 BDSG vorsieht, sah sich jedoch nicht in der Lage, die von den Datenschutzaufsichtsbehörden gesetzte Frist zur datenschutzgerechten Umgestaltung des HIS-Systems bis Ende 2008 einzuhalten. Zur Begründung führte der GDV an, dass er ein externes Unternehmen mit der Führung des neuen HIS beauftragen werde. Zu diesem Zwecke habe er eine Ausschreibung vorgenommen. Ende 2009 wurde der Zuschlag an ein in Baden-Württemberg ansässiges Unternehmen vergeben. Bei Redaktionsschluss waren die Vorbereitungen für die technische Umsetzung des neuen HIS noch nicht abgeschlossen. Nach Angaben des GDV soll der Wirkbetrieb im April 2011 beginnen.

Die HIS-Neukonzeption wurden zwischen den Datenschutzaufsichtsbehörden und dem GDV eingehend erörtert. Die Datenschutzaufsichtsbehörden können das neue HIS nur akzeptieren, wenn bestimmte Bedingungen erfüllt sind (vgl. Kasten zu Nr. 10.7).

Nachdem der GDV bereits einen „Compliance-Leitfaden“ erstellt hat, der noch mit den Datenschutzaufsichtsbehörden in der AG Versicherungswirtschaft abgestimmt werden soll, hoffe ich, dass die Verhandlungen zu einem erfolgreichen Abschluss gelangen und der leider noch immer bestehende datenschutzrechtswidrige Zustand auf der Grundlage des alten HIS im Frühjahr 2011 endlich beendet wird.

### Umgang mit Gesundheitsdaten

Bei bestimmten Versicherungsverträgen werden Gesundheitsdaten erhoben und verwendet, ohne dass dies durch eine gesetzliche Vorschrift ausdrücklich legitimiert würde. Für die Weitergabe von Daten, die der ärztlichen Schweigepflicht unterliegen, wird eine zusätzliche Legitimation eingeholt, beispielsweise bei der Einschaltung von externen medizinischen Gutachtern oder bei der Übermittlung

im Fall einer Auftragsdatenverarbeitung oder an Rückversicherer.

Rechtliche Grundlage für die Verarbeitung von Gesundheitsdaten sind derzeit §§ 3 Absatz 9, 28 Absatz 6 i. V. m. § 4a BDSG, 213 VVG, 203 StGB. Diese allgemeinen Regelungen reichen aber nicht aus, um den Versicherungsunternehmen einen zulässigen Umgang mit den Gesundheitsdaten im Rahmen der Antragsbearbeitung und Vertragsabwicklung zu ermöglichen. Deswegen holen diese von ihren Versicherungsnehmern eine Vielzahl von Einwilligungs- und Schweigepflichtentbindungserklärungen ein, die oftmals nicht den gesetzlichen Anforderungen entsprechen, so dass das informationelle Selbstbestimmungsrecht der Betroffenen nicht gewährleistet ist.

Daher bedarf es nach Auffassung der AG Versicherungswirtschaft ergänzender spezieller gesetzlicher Rechtsgrundlagen für den Umgang mit Gesundheitsdaten, die Einwilligungs- und Schweigepflichtentbindungserklärungen der Betroffenen entbehrlich machen. Für die Versicherungswirtschaft wären insbesondere Regelungen erforderlich, die die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten bei der Begründung, Durchführung und Beendigung eines Vertragsverhältnisses erlauben und auch Kriterien für eine Übermittlung von Gesundheitsdaten an Dritte zu bestimmten Zwecken, z. B. zur Risikoprüfung oder Prüfung der Leistungspflicht, zur Verhinderung des Versicherungsmissbrauchs oder bei einer Funktionsausgliederung bzw. Auftragsdatenverarbeitung enthalten. Darüber hinaus müsste aber auch § 203 StGB entsprechend ergänzt werden, vor allem durch eine Vorschrift über die Strafbarkeit unbefugten Offenbarens durch Dritte, an die Gesundheitsdaten übermittelt worden sind, ähnlich wie sie derzeit in § 203 Absatz 2a StGB für Datenschutzbeauftragte enthalten ist.

Die AG Versicherungswirtschaft hat sich in dieser Angelegenheit an die Bundesregierung gewandt. Eine Antwort ist bis Redaktionsschluss noch nicht eingegangen.

Ich unterstütze grundsätzlich das auf den Versicherungsbereich beschränkte Anliegen der AG Versicherungswirtschaft, muss aber darauf hinweisen, dass es sich nicht ausschließlich um ein versicherungsrechtliches Problem handelt. Aus meiner Sicht würde eine begrenzte branchenspezifische Regelung für die Versicherungswirtschaft den Blick auf vergleichbare datenschutzrechtliche Probleme in anderen Bereichen verstellen, für die ebenfalls eine gesetzliche Lösung gefunden werden müsste. Dazu zählen die vielen freien Berufe, in denen ein besonderes Berufsgeheimnis zu wahren ist (z. B. Ärzte, Rechtsanwälte, Steuerberater), und bei denen die Weitergabe von Gesundheitsdaten oder vergleichbarer sensibler Daten ebenfalls in Betracht kommen kann. Würde man für jeden Bereich spezielle Regelungen schaffen, würde dies zu einer nicht vertretbaren Zersplitterung datenschutzrechtlicher Regelungen für ein und denselben Erlaubnistatbestand führen. Zudem bestünde die Gefahr, dass unterschiedliche Anforderungen an eine Datenübermittlung gestellt werden könnten.

Kasten zu Nr. 10.7

**Datenschutzrechtliche Anforderungen an das neue HIS:**

- HIS wird als Auskunftei auf der Grundlage von § 29 BDSG ausgestaltet.
- Einmeldungen in die Auskunftei dürfen nur bei Vorliegen einer Rechtsvorschrift und nicht auf der Grundlage von Einwilligungserklärungen erfolgen.
- Die gespeicherten Daten dürfen nur beim Vorliegen eines berechtigten Interesses abgefragt werden.
- Es ist größtmögliche Transparenz für die Versicherungsnehmer und sonstige Betroffene herzustellen.
- Die Einmeldekriterien sind ständig zu evaluieren.
- Es muss eine Ombudsstelle eingerichtet werden, die bei versicherungsrechtlichen Zweifelsfragen eingeschaltet werden kann und diese Fragen klärt.
- Die Versicherer halten strenge Compliance-Regelungen ein.

## 10.8 Europaweite Autobahnmaut? Nur mit gutem Datenschutz!

*Europa wächst zusammen – die Mauterhebung soll künftig vereinfacht werden. Ohne Wechsel seines Mobilfunk-Anbieters kann man heutzutage weltweit telefonieren – bald soll es nach Vorstellungen der EU-Kommission ein solches „Roaming" auch bei der Mauterhebung geben.*

Seit Jahren beschäftigen mich datenschutzrechtliche Aspekte der elektronischen Mauterhebung (erstmalig ausführlich 19. TB Nr. 29.1). Aktuell stellt sich die Frage, ob die datenschutzfreundlichen deutschen Regelungen zur LKW-Maut gegebenenfalls durch die Umsetzung europarechtlicher Forderungen unterlaufen werden könnten.

Die Mitgliedstaaten sind aufgrund der Richtlinie 2004/52/EG vom 29. April 2004 über die Interoperabilität elektronischer Mautsysteme und der Entscheidung 2009/750/EG der Kommission vom 6. Oktober 2009 über die Festlegung der Merkmale des europäischen elektronischen Mautdienstes gehalten, die Voraussetzungen für die Einführung eines Europäischen Elektronischen Mautdienstes (EETS) zu schaffen. Um die elektronische Mauterhebung aller Arten von Straßenbenutzungsgebühren im gesamten gemeinschaftlichen Straßennetz zu ermöglichen, wird der Binnenmarkt für europäische Anbieter geöffnet. Erklärtes Ziel ist, eine Interoperabilität dahingehend herzustellen, dass ein Anbieter dem Nutzer einen Vertrag, ein Fahrzeuggerät und eine Rechnung zur Verfügung stellen kann. Der positive Effekt für den Nutzer (z. B. große Speditionen, die europaweite Touren fahren) soll sein, dass er künftig seinen EETS-Dienstleister selbst aussuchen und somit einem verbesserten Komfort bei gleichzeitiger Verringerung des administrativen Aufwandes erreichen kann. Der EETS soll die nationalen elektronischen Mautdienste in den Mitgliedstaaten ergänzen.

Das Bundesministerium für Verkehr, Bau und Stadtentwicklung (BMVBS) hat mich in einem sehr frühen Stadium der Umsetzung der europäischen Forderungen beteiligt. So war jeder Mitgliedstaat verpflichtet, bis zum 9. Juli 2010 eine internetbasierte Plattform (EETS-Register) mit allen für potentielle Anbieter wichtigen Informationen zur Verfügung zu stellen. Dieses Register wurde beim Bundesamt für Güterverkehr (BAG) eingerichtet. Ab dem 9. Oktober 2010 musste das Register auch alle rechtlichen und technisch-organisatorischen Vorgaben für das sog. EEMD-Gebiet, d. h. das für LKW mautpflichtige Streckennetz, sowie Informationen über die nationale Registrierungsstelle enthalten. Ferner müssen die registrierten EETS-Dienstleister mit Niederlassung in Deutschland und die zwischen Mauterheber (BAG) und EETS-Dienstleistern abgeschlossenen Verträge ersichtlich sein. Auf der Homepage www.bag.bund.de stehen nunmehr umfangreiche Informationen für jeden zur Verfügung.

Das BMVBS hatte mich im Vorfeld der Registereinrichtung um datenschutzrechtliche Beratung gebeten. Meine Empfehlungen haben im Dokument 4.1 „Mauterhebung im EETS-Gebiet ABMG und Mauttransaktionskonzept“, abrufbar auf der Website des BAG, Eingang gefunden. Die dort wiedergegebene ausdrückliche Erwähnung der engen Zweckbindungsregelungen des Autobahnmautgesetzes lässt mich hoffen, dass diese durch die Öffnung des Binnenmarktes nicht umgangen werden. Ich werde dieses Thema weiter beobachten und gegebenenfalls mit meinen europäischen Kollegen erörtern.

## 11 Gesundheit und Soziales

### 11.1 Gesetzliche Krankenversicherung

#### 11.1.1 Neue Wege in der vertragsärztlichen Versorgung – neue Herausforderungen für den Datenschutz

*Ärzte, die an besonderen Versorgungsformen teilnehmen, sind häufig auf die Hilfe privater Abrechnungsdienstleister angewiesen. Der Schutz der sensiblen Gesundheitsdaten der Versicherten muss dabei gewährleistet sein.*

Der Gesetzgeber hält die gesetzlichen Krankenkassen verstärkt dazu an, ihren Versicherten besondere Versorgungsformen anzubieten. Eine solche besondere Versorgungsform ist beispielsweise die „integrierte Versorgung“. Darin arbeiten verschiedene Akteure des Gesundheitswesens gemeinsam fach- und/oder sektorenübergreifend (ambulant und stationär) zusammen. Die „hausarztzentrierte Versorgung“ stellt eine weitere besondere Versorgungsform dar. Sie zeichnet sich dadurch aus, dass ein Hausarzt als erste Anlaufstelle für den Patienten sämtliche Behandlungsschritte koordiniert („Lotsenfunktion“). Die besonderen Versorgungsformen sollen die Qualität in der medizinischen Versorgung steigern, die Transparenz erhöhen und die Wirtschaftlichkeit verbessern.

Dabei werden bisweilen die bekannten, im Gesetz detailliert geregelten Abrechnungswege verlassen. Häufig werden sog. Selektivverträge abgeschlossen, die Inhalt und Vergütung der Versorgung über Verträge außerhalb der von den Kassenärztlichen Vereinigungen organisierten Regelversorgung („Kollektivvertrag“) individuell-vertraglich festlegen. Vertragspartner der Krankenkassen können vor allem Vertragsärzte und Gemeinschaften von Vertragsärzten sein. Die Teilnahme an diesen Versorgungsformen ist sowohl für den Arzt als auch für den Versicherten freiwillig.

Als datenschutzrechtlich problematisch erweist sich, dass die Ärzte innerhalb der vertraglich geregelten Versorgungsformen nicht auf die Kassenärztlichen Vereinigungen als abrechnende Stellen zurückgreifen können. Die Ärzte selbst verfügen aber oftmals nicht über die für die Leistungsabrechnung erforderliche Infrastruktur. Dies hat zur Folge, dass die Ärzte privatrechtlich organisierte Stellen mit der Leistungsabrechnung beauftragen. Diese Vorgehensweise hat das Bundessozialgericht (BSG) in seiner Entscheidung vom 10. Dezember 2008 (B 6 KA 37/07 R) für unzulässig erklärt, vor allem weil bereichsspezifische gesetzlichen Befugnisnormen für die Übermittlung der personenbezogenen Abrechnungsdaten fehlen. Nach Auffassung des Gerichts kann die Datenübermittlung auch nicht auf eine Einwilligungserklärung gestützt werden, da oftmals Zweifel an der Freiwilligkeit der Abgabe der Einwilligungserklärung bestehen. Das BSG räumte dem Gesetzgeber eine Frist von sechs Monaten zur Schaffung einer gesetzlichen Grundlage für die Fälle ein, in denen die Abrechnung der erbrachten Leistungen in der Praxis teilweise bereits durch private Abrechnungsstellen erfolgte.

Der Gesetzgeber hat diese Vorgaben mit der 15. Arzneimittelrechts-Novelle vom 17. Juni 2009 zunächst vorläufig umgesetzt, indem er mit den §§ 120 Absatz 6 und 295 Absatz 1b Sätze 5 bis 8 SGB V eine befristete Rechtsgrundlage für die Abrechnung verschiedener besonderer Versorgungsformen geschaffen hat. Im Rahmen des Gesetzgebungsverfahrens habe ich deutlich gemacht, dass ich in der Einführung besonderer Versorgungsformen eine sozial- und gesundheitspolitische Entscheidung sehe, die aber datenschutzrechtlich flankiert werden muss. Dies gelte auch für die Einschaltung privater Abrechnungsstellen. Wichtig ist mir allerdings, dass dabei das gesetzlich vorgegebene Schutzniveau für die Verarbeitung medizinischer Daten durch private Stellen dem für Sozialdaten geltenden Schutzniveau entspricht. Der Gesetzgeber ist dieser Forderung nachgekommen: Die Neuregelungen unterwerfen auch die privaten Stellen dem Sozialgeheimnis (§ 35 SGB I), sie erklären § 80 SGB X (Auftragsdatenverarbeitung) für entsprechend anwendbar und enthalten Vorgaben zur aufsichtsrechtlichen Kontrolle von Auftraggebern und Auftragnehmern.

Auf Grundlage der Befugnis aus §§ 73b, 295 Absatz 1b SGB V wurden mittlerweile zwischen verschiedenen Krankenkassen und Hausarztverbänden auf Landesebene (teilweise durch Schiedsverfahren) Verträge zur hausarztzentrierten Versorgung geschlossen. Dabei wurden jedoch vielfach die datenschutzrechtlichen Anforderungen nicht hinreichend berücksichtigt. Insbesondere entsprachen die Verträge, denen sich die Hausärzte, die an der hausarztzentrierten Versorgung teilnehmen wollen, unterwerfen müssen, nicht den Voraussetzungen des § 80 SGB X (vgl. auch Nr. 11.1.2 und 2.4). Unzureichend erscheinen mir insbesondere folgenden Vertragsinhalte:

- Obwohl den Ärzten die Rolle des Auftraggebers zugeschrieben wird, haben sie de facto keine hinreichenden Gestaltungsbefugnisse. So bestimmen die Hausärzteverbände, also die vermeintlichen Auftragnehmer, über die vertragliche Ausgestaltung des Auftragsverhältnisses (z. B. die Auswahl eines wiederum unterbeauftragten Rechenzentrums).
- Die Verträge verpflichten die Ärzte zur Nutzung einer bestimmten Software zur Datenübertragung an die Hausärzteverbände. Gleichzeitig verwehren sie den Ärzten die Kenntnis wesentlicher Funktionen der Software. Es ist daher zweifelhaft, ob die Ärzte wissen, welche genauen Daten sie mittels der Software an den Hausärzteverband weitergeben. Die Ärzte als eigentlich verantwortliche Stelle haben damit nicht die gesetzlich vorgeschriebene Kontrolle über die verarbeiteten Daten.
- Die Hausärzteverbände verfolgen mit den Daten auch eigene, über die Abrechnung hinausgehende Zwecke (etwa das Führen von Musterprozessen als Teil der ihnen obliegenden Interessenvertretung), die von der gesetzlichen Ermächtigungsgrundlage nicht erfasst sind.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) ist im Juli 2010 gegen einen derartigen Vertrag von zwischen in seiner Zuständigkeit liegenden Krankenkassen und dem Hausärzteverband Schleswig-Holstein mit einer Verfügung nach § 38 Absatz 5 BDSG vorgegangen. Es hat dem Hausärzteverband Schleswig-Holstein unter Androhung eines Zwangsgeldes untersagt, auf Grundlage des geschlossenen Vertrags von eingeschriebenen Hausärzten stammende Patientendaten weiterzugeben oder diese selbst zu nutzen. Gegen diese datenschutzrechtliche Anordnung hat sich der Hausärzteverband Schleswig-Holstein gerichtlich gewehrt. Das Verwaltungsgericht Schleswig hat einen Antrag auf vorläufigen Rechtsschutz gegen die Verfügung des ULD zurückgewiesen. Diese Entscheidung wurde inzwischen vom OVG Schleswig bestätigt.

Derzeit befinde ich mich – in Abstimmung mit den Datenschutzbehörden der Länder – in Gesprächen mit den Beteiligten mit dem Ziel, eine sowohl dem Datenschutz als auch den übrigen Interessen gerecht werdende Lösung herbeizuführen. Die befristeten Übergangsregelungen müssen vor deren Auslaufen im Sommer 2011 durch endgültige Rechtsgrundlagen ersetzt werden. Ich werde dem Gesetzgeber dabei beratend zur Seite stehen.

### 11.1.2 Neue Reglungen zur Auftragsdatenverarbeitung und zur Informationspflicht bei Datenschutzverstößen im Sozialrecht

*Mit der Neufassung des § 80 SGB X werden an Auftraggeber und Auftragnehmer bei der Verarbeitung von Sozialdaten im Auftrag strengere Anforderungen gestellt. Außerdem müssen sie über Datenschutzverstöße in ihrem Bereich informieren.*

Nach Inkrafttreten der strengeren Anforderungen an die Auftragsdatenverarbeitung in § 11 BDSG am 1. September 2009 (vgl. Nr. 2.4) lag das Schutzniveau für sensible Sozialdaten unter demjenigen für (bisweilen weniger sensible) Daten, die dem BDSG unterfallen, da eine entsprechende Änderung des SGB X unterblieben war. Auf diesen Wertungswiderspruch habe ich das zuständige Bundesministerium für Arbeit und Soziales (BMAS) aufmerksam gemacht und auf ein rasches gesetzgeberisches Handeln gedrängt.

Mit einer am 5. August 2010 verkündeten Gesetzesänderung (BGBl. I S. 1127) ist der Gesetzgeber dieser Forderung nachgekommen. Der neu gefasste § 80 Absatz 2 Satz 2 SGB X legt nun detailliert fest, welche Anforderungen bei der Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag beachtet werden müssen. Der Auftraggeber wird außerdem verpflichtet, sich regelmäßig von der Einhaltung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen und das Ergebnis der Prüfung zu dokumentieren. § 80 Absatz 2 Satz 2 SGB X entspricht damit § 11 Absatz 2 BDSG.

Zudem verpflichtet der neue § 83a SGB X die dem Sozialgeheimnis unterliegenden Stellen, im Fall der unrechtmäßigen Kenntniserlangung von Sozialdaten unverzüglich die Aufsichtsbehörde nach § 90 SGB IV, die zuständige Datenschutzaufsichtsbehörde und den Betroffenen zu informieren. Im Hinblick auf die Art der Benachrichtigung verweist die Norm auf § 42a BDSG. Erste Meldungen über Datenschutzverstöße aufgrund dieser neuen Vorschrift haben mich bereits erreicht.

Ebenfalls den BDSG-Regelungen nachempfunden ist die Bußgeldbewehrung von Verstößen gegen die Vorschriften über die Auftragsdatenverarbeitung und die Informationsverpflichtung.

### 11.1.3 Elektronischer Entgeltnachweis

#### 11.1.3.1 Das ELENA-Verfahren

*Mit dem im Frühjahr 2009 beschlossenen ELENA-Verfahrensgesetz wurde nach langer Diskussion eines der größten Datenverarbeitungsvorhaben im Sozialbereich gesetzlich geregelt. Letztlich wird das Bundesverfassungsgericht (BVerfG) über seine Verfassungsmäßigkeit zu entscheiden haben.*

Seit vielen Jahren habe ich fortlaufend über das Vorhaben der Bundesregierung berichtet, für die Erstellung von Einkommensnachweisen erforderliche Daten aller Beschäftigten bei einer zentralen Stelle zu speichern und diese für Sozialbehörden zur Entscheidung etwa über Sozialleistungen elektronisch verfügbar zu machen (vgl. etwa 19. TB Nr. 23.2.2; zuletzt 22. TB Nr. 6.2).

Durch das ELENA-Verfahrensgesetz vom 28. März 2009 (BGBl. I S. 634) wurde mir die Verwaltung des Datenbank-Hauptschlüssels nach § 99 Absatz 3 Satz 2 SGB IV zugewiesen. Der Bundestag hat meine Bedenken, durch diese Aufgabenzuweisung könnte die Unabhängigkeit des BfDI beeinträchtigt werden, da es sich bei der Schlüsselverwaltung letztlich um eine Verwaltungsaufgabe handele, nicht berücksichtigt. Diese Aufgabenübertragung enthält

detaillierte Vorgaben zur IT-Sicherheit (vgl. u. Nr. 11.1.3.2).

Aufgrund der gesetzlichen Vorgaben ist zum 1. Januar 2010 zunächst lediglich die Verpflichtung zur Zulieferung von Daten für das ELENA-Verfahren in Kraft getreten (vgl. Kasten zu Nr. 11.1.3.1). Seit diesem Zeitpunkt sind die Arbeitgeber verpflichtet, Daten ihrer Arbeitnehmer an die Zentrale Speicherstelle (ZSS) zu melden. Die ZSS ist räumlich, organisatorisch und personell getrennt bei der Datenstelle der Träger der Rentenversicherung eingerichtet worden (§ 96 Absatz 1 SGB IV). Ende des Jahres 2010 hatte die Registratur Fachverfahren (RFV) 33 126 688 vorläufige Identitätsnummern für ebenso viele Arbeitnehmer vergeben. Insgesamt waren damit am 31. Dezember 2010 ca. 330 Millionen Datensätze gespeichert.

Die einzumeldenden Daten sind in einem sogenannten Multifunktionalen Verdienstdatensatz (MVDS) festgelegt, der aus verschiedenen Datenbausteinen besteht, die teilweise monatlich, teilweise anlassbezogen gemeldet werden müssen.

Einer dieser anlassbezogen zu meldenden Datenbausteine ist der Datenbaustein Kündigung/Entlassung, der im Berichtszeitraum im Fokus des Interesses stand, weil er vorsah, dass im Falle der Kündigung u. a. auch gemeldet werden sollte, ob der Kündigung die Teilnahme an einem Streik oder einer Aussperrung zugrunde lag. Nicht zuletzt aufgrund meiner Intervention wurde der Datenbaustein so geändert, dass diese Informationen über das ELENA-Verfahren nicht erhoben werden. Außerdem konnte ich erreichen, dass die Arbeitgeber keine sogenannten Freitextfelder mehr ausfüllen müssen, da dies die Gefahr beinhaltet hätte, dass unsachliche Freitexte Einfluss auf die Vergabe von Sozialleistungen an Bürger gehabt hätten.

Gegen Ende des Berichtszeitraumes wurden Pläne der Regierungskoalition bekannt, das verbindliche Abrufverfahren statt am 1. Januar 2012 erst am 1. Januar 2014 beginnen zu lassen. Die Gründe liegen zum einen in der Nichtverfügbarkeit der erforderlichen Karten mit einer qualifizierten elektronischen Signatur, zum anderen fehlt es bei den abrufenden Stellen aber auch noch an den technischen Möglichkeiten für den Abruf. Nicht ändern soll sich allerdings die Regelung, wonach zu Erprobungszwecken auch bereits vor dem festgesetzten Termin ein Abruf möglich sein soll.

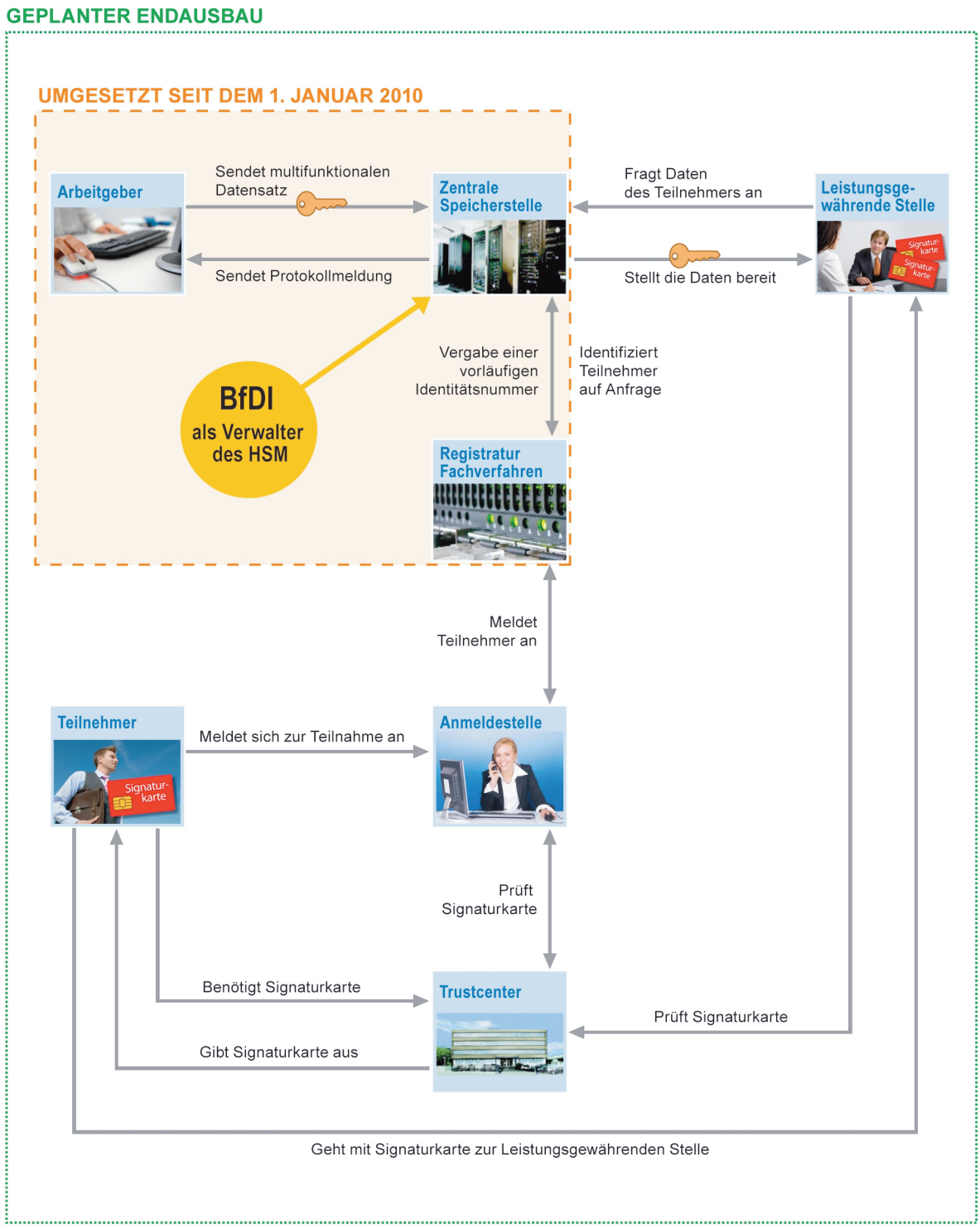
Diese Regelung ist insbesondere erforderlich, um möglichst schnell den Anspruch auf Selbstauskunft nach § 103 Absatz 4 Satz 1 SGB IV zu realisieren. Diese Vorschrift gibt den Bürgern einen Auskunftsanspruch gegenüber der ZSS und der Registratur Fachverfahren über die dort zu ihrer Person gespeicherten Daten. Der Anspruch ist jedoch bei der ZSS derzeit nicht umsetzbar, weil die ZSS aufgrund datenschutzrechtlicher Vorgaben keinen Zugang zu den bei ihr gespeicherten Daten hat. Durch diese Vorgabe soll bereits technisch verhindert werden, dass die ZSS von außen dazu genötigt werden könnte, Daten herauszugeben. Aus diesem Grund war in den vorangegangenen JobCard-Projekten großer Wert darauf gelegt worden, dass der Auskunftsanspruch nur über eine abrufende Behörde gestellt werden konnte. Hierdurch sollte innerhalb des ELENA-Verfahrens das Zwei-Signaturen-Prinzip sichergestellt werden, nach welchem für einen Abruf aus der ELENA-Datenbank stets zwei elektronische Signaturen erforderlich sind, nämlich die qualifizierte elektronische Signatur des Teilnehmers und die elektronische Signatur der abrufenden Behörde nach § 102 SGB IV. Dieser wesentlichen datenschutzrechtlichen Sicherung steht allerdings § 103 Absatz 4 Satz 3 Alt. 2 SGB IV entgegen, wonach der Anspruch auch direkt gegenüber der ZSS geltend gemacht werden kann. Mit den am ELENA-Verfahren beteiligten Stellen erarbeite ich derzeit eine Möglichkeit, den Auskunftsanspruch zu verwirklichen, ohne dass wesentliche Sicherheitsmaßnahmen des ELENA-Verfahrens außer Kraft gesetzt werden müssen.

Im Berichtszeitraum habe ich eine erste datenschutzrechtliche Kontrolle der ZSS durchgeführt. Dabei habe ich festgestellt, dass die in § 96 Absatz 1 SGB IV vorgesehene räumliche Trennung der ZSS von der Datenstelle der Träger der Rentenversicherung (DSRV) zwar verwirklicht wurde, es aber noch Defizite bei der gesetzlich geforderten organisatorischen und personellen Trennung gibt. Insbesondere halte ich das Weisungsrecht gegenüber den Mitarbeitern der ZSS durch Vorgesetzte der DSRV mit den gesetzlichen Vorgaben nicht vereinbar. Der Hinweis auf nicht näher spezifizierte finanzielle Probleme bei der Beachtung der gesetzlichen Vorgaben darf jedenfalls nicht dazu führen, dass diese nicht beachtet werden.

Zu den vor dem Bundesverfassungsgericht (BVerfG) anhängigen Verfassungsbeschwerden gegen das ELENA-Verfahren habe ich ebenfalls Stellung genommen. Mit Beschluss vom 14. September 2010 (1 BvR 872/10) hat es das BVerfG abgelehnt, durch eine einstweilige Anordnung die §§ 97 Absatz 1 und 98 Absatz 1 SGB IV auszusetzen, die die Meldepflicht der Arbeitgeber und die Anmeldepflicht der Teilnehmer betreffen. Ein wesentlicher Aspekt, über den das BVerfG im Hauptsacheverfahren zu entscheiden hat, wird die Frage sein, ob das ELENA-Verfahren eine unzulässige Datenvorratshaltung darstellt (vgl. hierzu schon 19. TB Nr. 23.2.2, S. 131). Ich gehe davon aus, dass das BVerfG die in seiner Entscheidung vom 2. März 2010 zur Vorratsdatenspeicherung von Telekommunikationsdaten herausgearbeiteten Kriterien auf das ELENA-Verfahren anwenden wird (vgl. o. Nr. 6.1), und halte das ELENA-Verfahren nur dann für verfassungsgemäß, wenn das Sicherheitsniveau auf dem Standard bleibt, wie es während der JobCard-Projekte und des Gesetzgebungsverfahrens zum ELENA-Verfahrensgesetz verabredet wurde. Bestrebungen, etwa aus Kostengründen hiervon Abstriche zu machen, werde ich mich weiterhin entgegen stellen.

Kasten zu Nr. 11.1.3.1

## Funktionaler Ablauf des ELENA-Verfahrens



#### 11.1.3.2 ELENA – Das Sicherheitskonzept für den Datenbank-Hauptschlüssel

*Das Gesetz über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) wurde am 28. März 2009 im Bundesgesetzblatt (BGBl. 2009 I S. 634) verkündet. Damit wurde mir die neue Aufgabe zugewiesen, den Datenbank-Hauptschlüssel zu verwalten. Die Verwaltung des Schlüssels soll das Verfahren ELENA sicherer machen und ist ein wesentlicher Teil eines umfassenden komplexen Sicherheitskonzepts.*

Nach § 99 Absatz 3 SGB IV wird der Datenbank-Hauptschlüssel durch meine Dienststelle verwaltet. Einzelheiten regelt das Gesetz nicht. Diese Aufgabe kann aufgrund der Vorprojekte und der Konzeption des ELENA-Verfahrens (vgl. hierzu u. Nr. 11.1.3.1) wie folgt beschrieben werden:

Die Funktion des Datenbank-Hauptschlüsselverwalters wurde zur Stärkung des Datenschutzes geschaffen. Da die Sitzungsschlüssel (Sessionskeys) für einzelne Datensätze mit dem Hauptschlüssel (Masterkey) verschlüsselt sind, erhält der Betreiber der ELENA-Datenbank – das ist die bei der Datenstelle der Träger der Rentenversicherung eingerichtete Zentrale Speicherstelle (ZSS) – nicht gleichzeitig auch die Hoheit über den Inhalt der Datenbank. Die Datenbankinhalte können nur durch Freigabe des Datenbank-Hauptschlüsselverwalters gelesen werden. Für die Verschlüsselung des Sitzungsschlüssels der schützenswerten Daten in der ZSS ist der Einsatz eines Hardware Security Moduls (HSM) vorgesehen. Bei dem HSM handelt es sich um eine speziell geschützte und zertifizierte Hardware für kryptographische Operationen, die höchsten Sicherheitsanforderungen genügt. Meine Aufgaben umfassen neben der Administration des HSM auch die Überwachung der Abrufe aus der Datenbank.

Im Einzelnen habe ich als Datenbank-Hauptschlüsselverwalter folgende Aufgaben:

- Erarbeitung und Fortschreibung eines Kryptokonzepts (unter Beteiligung des BSI)
- Betrieb des HSM, in denen der Datenbank-Hauptschlüssel (Masterkey) der ZSS generiert, verwaltet und gespeichert wird
- Verwahrung des Backups des (Ersatz-) Datenbank-Hauptschlüssels (Masterkeys) für den Fall eines Defektes im laufenden System
- Initiierung von planmäßigen (jährlichen) und außerplanmäßigen Schlüsselwechseln sowie deren Durchführung und Dokumentation
- Überwachung des Betriebs der ZSS und der Zugriffe auf den Datenbank-Hauptschlüssel
- Beantwortung von Auskunftsersuchen von Behörden und Privatpersonen
- Aktive Mitwirkung beim Betrieb der ZSS zur Überwachung von sicherheitsrelevanten Aktivitäten
- „Tätige Zwei-Augen“ als Unterstützung des Vier-Augen-Prinzips bei der Anmeldung von Verantwortlichen der abrufenden Stellen
- Überwachung der Rechtmäßigkeit der Abrufe aus der Datenbank (in Verbindung mit den Landesbeauftragten für den Datenschutz)

Seit dem 1. Januar 2010 sind die Arbeitgeber nach dem ELENA-Verfahrengesetz verpflichtet, die Entgeltdaten zu melden. Daher standen zunächst die Installation und die Aufnahme des Betriebs eines HSM im Vordergrund. Hierfür habe ich zusammen mit der ZSS ein HSM-Betriebskonzept erarbeitet. Dabei sind die Beschaffung und Inbetriebnahme in enger Abstimmung mit der ZSS erfolgt, da die Systemkomponenten aufeinander abgestimmt werden mussten. Mit Hilfe des in dem HSM gespeicherten Datenbank-Hauptschlüssels werden alle Sitzungsschlüssel (Sessionkeys), mit denen die Datensätze in der ZSS-Datenbank verschlüsselt werden, wiederum verschlüsselt. Dies bedeutet:

Ohne meine Mitwirkung kann kein Datensatz der ELENA-Datenbank entschlüsselt werden. Da das HSM im Monat ca. 34 Millionen Datensätze jeweils mit einem anderen Sessionkey zu verschlüsseln hat, sind sehr hohe Performanz- und Sicherheitsanforderungen zu stellen.

Im Laufe des Jahres 2009 wurde das HSM beschafft und in Betrieb genommen. Rechtzeitig vor der Meldung der ersten Entgeltdaten wurde im Dezember 2009 durch zwei Mitarbeiter meiner Dienststelle der Datenbank-Hauptschlüssel „2010“ generiert.

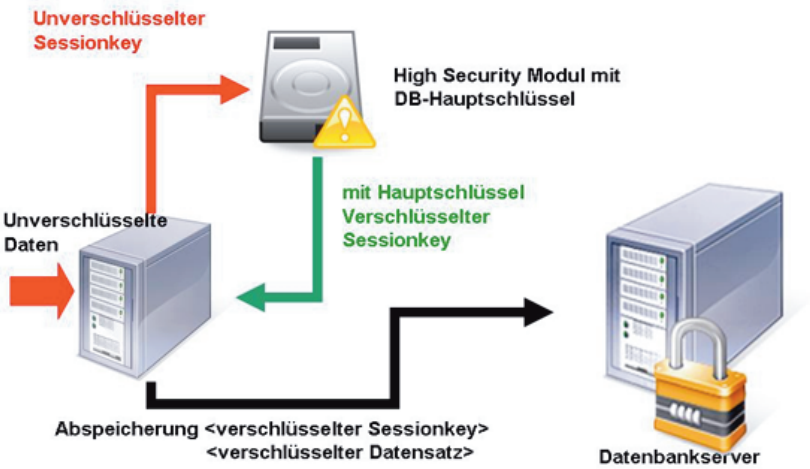
Das HSM ist physikalisch im Rechenzentrum der Zentralen Speicherstelle (vgl. Kasten zu Nr. 11.1.3.2) untergebracht. Zugriff auf diese Systeme ist nur von autorisierten Mitarbeitern des BfDI vor Ort möglich. Eine externe Schnittstelle (Online-Verbindung) wurde aus Sicherheitsgründen nicht eingerichtet.

Für das HSM wurde ein Grobkonzept, ein Sicherheitskonzept und ein Betriebskonzept erarbeitet und dem BSI zur Prüfung vorgelegt. Diese werden den jeweiligen Anforderungen entsprechend fortgeschrieben.

Wenn die abrufenden Stellen ihren Betrieb aufnehmen und in das ELENA-System eingebunden werden, muss die Entschlüsselung der Daten in dem HSM ebenfalls berücksichtigt werden. Ich bin daher auch nach dem Aufbau der Infrastruktur weiterhin in das Verfahren intensiv eingebunden.

Kasten zu Nr. 11.1.3.2

**Verschlüsselung in der Zentralen Speicherstelle**




### 11.1.4 Mangelhaft geschützte Daten bei der Aufgabenwahrnehmung durch private Callcenter

*Ein Kontrollbesuch bei einer gesetzlichen Krankenkasse offenbarte schwerwiegende datenschutzrechtliche Verstöße bei der Zusammenarbeit mit einem privaten Dienstleistungsunternehmen.*

In meinem letzten Tätigkeitsbericht (22. TB Nr. 10.2.2) hatte ich die datenschutzrechtlichen Gefahren aufgezeigt, die im Zusammenhang mit der verstärkt bei Sozialversicherungsträgern zu beobachtenden Tendenz stehen, ihnen obliegende Aufgaben an private Dienstleistungsunternehmen zu übertragen. Der Kontrollbesuch bei einer gesetzlichen Krankenkasse offenbarte erhebliche Datenschutzverstöße.

Der Kontrollbesuch fand statt, nachdem ich durch Medienanfragen, die ihrerseits auf Insider-Tipps beruhten, Hinweise auf Datenschutzverstöße erhalten hatte. Die geprüfte Krankenkasse betreibt zur Kundenkommunikation ein hauseigenes Callcenter. Um der ganztägigen Servicenachfrage ihrer Versicherten gerecht zu werden, beauftragte die Kasse ein Privatunternehmen, Anrufspitzen in den Abend- und Nachtstunden abzufangen und in Zeiten hohen Anrufaufkommens das interne Callcenter zu entlasten. Das von der Kasse beauftragte Unternehmen (A) beauftragte einen anderen privaten Dienstleister (B), der wiederum sein Schwesterunternehmen (C) mit der Erbringung von Teilen der Leistungen, die gegenüber der Krankenkasse geschuldet waren, beauftragte (vgl. Kasten zu Nr. 11.1.4). Erbracht wurde die Callcenter-Tätigkeit letztlich durch selbständige Berater, die sich hierzu – teilweise neben anderen Projekten – gegenüber dem Unternehmen C vertraglich verpflichteten. Insgesamt waren für die Krankenkasse zwischen 70 und 80 selbständige Berater tätig, die vor Aufnahme ihrer Tätigkeit eine von der Kasse organisierte einwöchige Schulung zu durchlaufen hatten. Das dabei zur Verfügung gestellte Lehrmaterial zur Veranschaulichung des Arbeitsablaufs enthielt keine fiktiven, sondern personenbezogene Daten (u. a. Namen, Adressen, Bankverbindungen und medizinische Daten) von Versicherten der Krankenkasse.

Anlässlich der Kontrolle habe ich festgestellt, dass die behördliche Datenschutzbeauftragte der Krankenkasse in das Verfahren, insbesondere in die Vertragsgestaltungen, welche die (Unter-)Auftragsverarbeitung besonders sensibler Sozialdaten zum Inhalt hatten, zu keinem Zeitpunkt eingebunden war. Die erforderliche datenschutzrechtliche Vorabkontrolle war ebenfalls nicht erfolgt. Auch nach Auftragserteilung an das Unternehmen A fand keine datenschutzrechtliche Kontrolle des Dienstleisters durch die Krankenkasse statt. Außerdem habe ich bemängelt, dass die Krankenkasse am Tag des Kontrollbesuchs weder ein aktuelles Verfahrensverzeichnis noch ein ausreichendes IT-Sicherheitskonzept vorlegen konnte.

Die externen Berater erbrachten die vertraglich vereinbarte Dienstleistung von ihrem privaten häuslichen Computer aus. Sie hatten dabei über das Internet Zugriff auf Daten der Versicherten, die auf einem System der Kasse gespeichert waren. Dabei wurden keine – technisch durchaus möglichen – Maßnahmen zur Vermeidung eines möglichen Zugriffs auf Versichertendaten durch unbefugte Dritte getroffen. Durch eine von der Krankenkasse zugeteilte Kennung (Benutzer-ID, Passwort) erhielten die Berater Zugang auf die Datensysteme der Krankenkasse. Eine Zugangsbeschränkung auf den konkreten Zeitpunkt einer Versichertenanfrage existierte nicht. Lediglich eine Zwangstrennung des externen Zugangs in den Nachtstunden zur Verhinderung automatisierter Datenabrufe war eingerichtet.

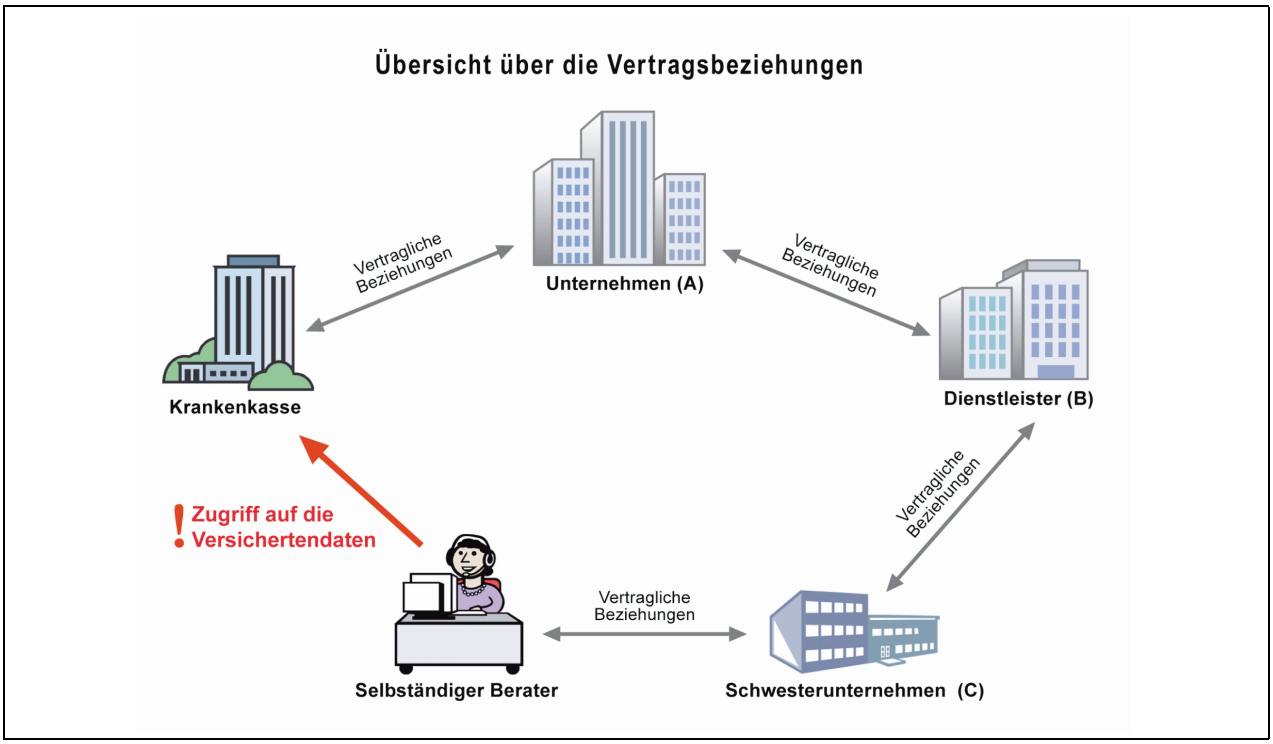
Je nach Qualifikation wurden die Berater für den „First Level Support“ (einfache Versichertenanfragen) oder den „Second Level Support“ (anspruchsvollere Anfragen) eingesetzt. Dabei hatten jedoch sämtliche Berater undifferenzierten Zugriff auf den gesamten Versichertendatenbestand einschließlich besonders sensibler Gesundheitsdaten. Der Zugriff erstreckte sich neben Namen, Anschrift und Alter aller bei der Krankenkasse Versicherten auch auf deren Bankverbindungen, Angaben über medizinische Leistungen, Diagnosen chronischer Erkrankungen, den behandelnden Arzt und Krankengeldbezug. Diese unbeschränkte Zugriffsmöglichkeit auf den gesamten Versichertendatenbestand der Krankenkasse war für die Erbringung der vertraglich festgelegten Leistungen weder erforderlich noch wurde dem gebotenen Zugriffsschutz in irgendeiner Weise Rechnung getragen.

Der Zugriff der externen Berater auf den Datenbestand der Krankenkasse erfolgte innerhalb des von Dienstleister C verwendeten Systems. Die freien Mitarbeiter wählten sich über eine verschlüsselte und abgesicherte Verbindung (VPN-Tunnel) bei einem Rechenzentrum des Unternehmens C ein. Der dortige Server war mit dem Datensystem der Krankenkasse verbunden. Neben der Verschlüsselung und dem VPN-Tunnel existierten keine weiteren Sicherheitsvorkehrungen auf den Rechnern der Berater. Durch die Sicherheitsrichtlinien der Systemadministration (Sperrung von lokalem Laufwerk, CD-Brenner, USB und Druckerschnittstellen) konnte aber zumindest sichergestellt werden, dass keine den Systemen der Krankenkasse entnommenen Daten lokal am externen PC gespeichert oder ausgedruckt werden konnten. Ein Kopieren der Daten oder das Mitlaufen eines sog. Loggers waren deshalb nach bisherigem Wissenstand nicht möglich, jedoch konnten einzelne Maskeninhalte (Screenshots) eines Versichertenkontos lokal am externen PC abgespeichert, gedruckt oder in eine andere Datei exportiert werden.

Aufgrund dieser erheblichen Mängel bei den technischen und organisatorischen Maßnahmen zum Schutz der sensiblen Sozialdaten habe ich gegenüber dem Vorstand der Krankenkasse insgesamt fünf datenschutzrechtliche Beanstandungen ausgesprochen. Hervorheben möchte ich aber auch das äußerst kooperative Verhalten der Krankenkasse während und nach meinem Kontrollbesuch. Insbesondere begrüße ich, dass umgehend weitreichende Maßnahmen zur Sicherstellung des Datenschutzes ergriffen wurden.

Trotzdem bleibt ein schaler Beigeschmack: Die festgestellten Zustände verstießen in eklatanter Weise gegen datenschutzrechtliche Vorgaben und setzten sensible personenbezogene Daten in unverantwortlicher Weise vermeidbaren Risiken aus. Wie oben ausgeführt, wurde meine Prüfung durch Hinweise ausgelöst, die ich von anderer Seite erhalten hatte. Es ist nicht ausgeschlossen, vielleicht sogar wahrscheinlich, dass es sich nicht um einen Einzelfall handelt. Vielmehr drängt sich mir der Eindruck auf, dass eine einseitige Fokussierung auf wirtschaftliche Kenngrößen sich negativ auf den Datenschutz auswirkt. Dies betrifft auch – aber nicht nur – die Krankenversicherungen, jedenfalls soweit sie im Wettbewerb stehen. Ich möchte deshalb daran erinnern, dass letztlich immer die Geschäftsleitungen die Verantwortung für den Umgang mit personenbezogenen Daten haben. Die Gewährleistung des Datenschutzes – insbesondere bei sensiblen Daten – ist Chefsache und darf nicht auf Mitarbeiter, Auftragnehmer oder sonstige Vertragspartner abgewälzt werden.

Kasten zu Nr. 11.1.4



### 11.1.5 Verfahren zur Erhebung von Zusatzbeiträgen und Datenerhebung zum Sozialausgleich – das GKV-Finanzierungsgesetz

*Das GKV-Finanzierungsgesetz ermöglicht den gesetzlichen Krankenkassen die Erhebung einkommensunabhängiger Zusatzbeiträge in unbegrenzter Höhe. Beim Sozialausgleich, der den Beitragszahler vor finanzieller Überforderung schützen soll, ist auch der Datenschutz gefragt.*

Mit dem Ende 2010 beschlossenen GKV-Finanzierungsgesetz (BGBl. I S. 2309) erhalten die gesetzlichen Krankenkassen die Möglichkeit, individuelle Zusatzbeiträge zu erheben. Die Zusatzbeiträge müssen von den Mitgliedern unabhängig von ihrem Einkommen gezahlt werden. Als Kompensation für den Wegfall der bisherigen Überforderungsklausel wurde ein Sozialausgleich eingeführt, der den Beitragszahler vor einer unverhältnismäßigen finanziellen Belastung schützen soll. Dieser Sozialausgleich wird für Arbeitnehmer und Rentner über die Arbeitgeber bzw. Rentenversicherungsträger im Rahmen der elektronischen Abrechnung von Löhnen, Gehältern und Renten durchgeführt, indem der Zusatzbeitrag um die jeweils berechnete Überlastung durch den durchschnittlichen Zusatzbeitrag reduziert wird. Außerdem dürfen die Krankenkassen nun einen Säumniszuschlag bei denjenigen Versicherten erheben, die mit der Zahlung des Zusatzbeitrags für mindestens sechs Kalendermonate säumig sind.

Ein früherer Entwurf des Gesetzes sah dazu vor, dass die zuständige Krankenkasse im Falle der Säumnis des Beitragszahlers die den Beitrag abführende Stelle zu informieren hat, dass kein Sozialausgleich mehr durchgeführt werden soll. Sobald die ausstehenden Beiträge und Säumniszuschläge vollständig gezahlt werden, sollte die Kasse die abführende Stelle auch darüber informieren. Dagegen habe ich datenschutzrechtliche Bedenken gegenüber dem Bundesministerium für Gesundheit (BMG) geäußert. Die Kenntnis eines Zahlungsrückstandes eines Arbeitnehmers hätte dem Arbeitgeber weitgehende Einblicke in die Zahlungsmoral seines Beschäftigten gegeben. Er hätte daraus Rückschlüsse – ob richtig oder falsch – auf die finanzielle Situation des säumigen Beitragszahlers ziehen können. Meinen Bedenken hat das BMG insoweit Rechnung getragen, als dass die Krankenkassen den beitragsabführenden Stellen nunmehr ohne Angabe von Gründen Beginn und Ende des Zeitraums mitteilen, in dem der Sozialausgleich durchzuführen ist. Damit erhält der Arbeitgeber keine Informationen über die Gründe, warum er den Sozialausgleich nicht mehr bzw. wieder durchzuführen hat.

Mit der den Krankenkassen neu auferlegten Aufgabe der Durchführung des Sozialausgleichs wurde aus datenschutzrechtlicher Sicht außerdem eine Ergänzung des Aufgabenkatalogs des § 284 Absatz 1 SGB V erforderlich. Dieser legt abschließend fest, zu welchen Zwecken Krankenkassen Sozialdaten erheben, verarbeiten und nutzen dürfen. Meine Forderung, eine ausdrückliche Befugnisnorm für die mit der Durchführung des Sozialausgleichs einhergehende Datenerhebung, -verarbeitung und -nutzung zu schaffen, hat der Gesetzgeber damit umgesetzt.

Kritisch sehe ich es weiterhin, dass der Arbeitgeber im Rahmen des von ihm durchzuführenden Sozialausgleichs Kenntnis darüber erlangt, ob ein Beschäftigter über weitere beitragspflichtige Einnahmen verfügt, obwohl der Betroffene unter Umständen ein Interesse an der Geheimhaltung dieser Information hat. Leider konnte ich aber mit meiner Anregung nicht durchdringen, den Sozialausgleich innerhalb des Steuersystems ohne Zwischenschaltung des Arbeitgebers durchzuführen.

So ist die Neuregelung ein Beispiel dafür, dass an sich zu Gunsten von Betroffenen gedachte Maßnahmen bisweilen negative datenschutzrechtliche Nebenwirkungen haben.

### 11.1.6 Das Sparschwein in der Mitgliederzeitschrift und die Erhebung der Steuer-ID durch die gesetzliche Krankenkasse

*Gesetzliche Krankenkassen müssen ihre Versicherten im Voraus schriftlich informieren, wenn sie deren Steuer-ID beim Bundeszentralamt für Steuern (BZSt) abfragen, um Daten an die Finanzbehörden zu übermitteln. Den betroffenen Versicherten wird hierdurch die Möglichkeit zum Widerspruch gegeben. Ein bloßer Hinweis in der Mitgliederzeitschrift genügt nicht.*

Durch das seit dem 1. Januar 2010 geltende „Bürgerentlastungsgesetz Krankenversicherung“ vom 16. Juli 2009 (BGBl. I S. 1959) können Beiträge zur privaten und gesetzlichen Kranken- und Pflegeversicherung (Vorsorgeaufwendungen) steuerlich stärker als bisher berücksichtigt werden. Die steuerliche Berücksichtigung setzt allerdings voraus, dass die Finanzämter Informationen über die Höhe der berücksichtigungsfähigen Kranken- bzw. Pflegeversicherungsbeiträge erhalten. Im Regelfall meldet der Arbeitgeber die Daten zusammen mit der elektronischen Lohnsteuerbescheinigung an die Finanzämter. Über bestimmte Beiträge wie beispielsweise die von Selbstständigen geleisteten Krankenkassenbeiträge oder die Zusatzbeiträge haben die Finanzämter hingegen keine Informationen.

Um auch diese „Selbstzahler“ in den Genuss der Steuervergünstigung kommen zu lassen, platzierte eine gesetzliche Krankenkasse in ihrer Mitgliederzeitschrift einen mit einem Sparschwein dekorierten Hinweis, dass sie die steuerlich absetzbaren Beiträge ihrer Versicherten direkt an das Finanzamt melde. Die hierfür erforderliche Steuer-ID (vgl. Nr. 9.2) ihrer Mitglieder werde sie bei der BZSt erfragen, falls die Versicherten nicht widersprächen.

Die Idee war gut gemeint, ist datenschutzrechtlich aber gleich aus mehreren Gründen problematisch:

Es ist zweifelhaft, ob die gesetzlichen Vorschriften des Einkommensteuergesetzes überhaupt eine tragfähige Rechtsgrundlage für die Erhebung der Steuer-ID durch die Krankenkassen sein können. Zwar erlaubt das Einkommensteuergesetz grundsätzlich eine Abfrage der Steuer-ID beim BZSt ohne Einwilligung des Betroffenen, allerdings gilt im vorliegenden Zusammenhang die Besonderheit, dass die Steuer-ID hier als Sozialdatum zu behandeln ist, weil sie von der gesetzlichen Krankenversi-

cherung in Erfüllung einer Aufgabe nach dem Sozialgesetzbuch (§ 67 Absatz 2 Nr. 4 SGB X) erhoben wird.

Zudem können die Vorsorgeaufwendungen nur dann in vollem Umfang steuerlich berücksichtigt werden, wenn der versicherte Steuerpflichtige gegenüber dem Träger der gesetzlichen Krankenversicherung in die Datenübermittlung an die Finanzbehörde schriftlich eingewilligt hat. Aufgrund einer gesetzlichen Übergangsregelung gilt die Einwilligung zwar bei Verträgen, die vor dem 1. Januar 2011 begründet waren, unter bestimmten Bedingungen als erteilt. Diese Fiktion der Einwilligung setzt aber voraus, dass die Krankenkasse jeden Versicherten vor der Erhebung der Steuer-ID beim BZSt und vor der Übermittlung der Beitragsdaten an das zuständige Finanzamt schriftlich über ihr Vorgehen informiert und der Versicherte gegenüber der Krankenkasse nicht innerhalb von vier Wochen nach Erhalt der Information schriftlich widersprochen hat. Der Hinweis in der Mitgliederzeitschrift genügte diesen Anforderungen nicht. Nicht alle Versicherten werden die Zeitschrift lesen, und kaum ein Leser wird sich der rechtlichen Folgen des Verzichts auf sein Widerspruchsrecht bewusst sein. Die Warnfunktion der gesetzlich vorgeschriebenen Schriftform kann nicht erfüllt werden. Dieser genügt nur ein persönliches Schreiben an den Betroffenen. Aufgrund meines Hinweises hat die Krankenkasse das Verfahren mittlerweile umgestellt.

Datenschutzrechtlich bedenklich ist meiner Ansicht nach auch die Freiwilligkeit der Einwilligung und Einwilligungsfiktion. Den Steuerpflichtigen steht keine Alternative des Nachweises der gemachten Vorsorgeaufwendungen zur Verfügung, beispielsweise durch Vorlage von entsprechenden Bescheinigungen beim Finanzamt. Das BMF ist meinen Bedenken bislang jedoch nicht gefolgt (vgl. Nr. 9.2).

### 11.1.7 Protokollierungsempfehlungen für die Gesetzliche Krankenversicherung

*Die Arbeitskreise Technik sowie Gesundheit und Soziales der Datenschutzkonferenz haben „Empfehlungen zur Protokollierung in zentralen IT-Verfahren der Gesetzlichen Krankenversicherung“ erarbeitet.*

Änderungen der rechtlichen Rahmenbedingungen im Gesundheitswesen, die Erweiterung funktionaler Anforderungen, Fusionen von Krankenkassen sowie die technische Entwicklung haben im Bereich der Gesetzlichen Krankenversicherung (GKV) zu einer grundlegenden Weiterentwicklung der eingesetzten IT-Verfahren geführt. Angesichts der Komplexität der eingesetzten Großverfahren bedarf es für eine datenschutzgerechte Gestaltung eines geeigneten Instrumentariums, um die Verarbeitung personenbezogener Daten – etwa bei datenschutzrechtlichen Prüfungen – nachvollziehen zu können. Dies gilt besonders für den Bereich der GKV wegen der Sensibilität der verarbeiteten Gesundheits- und Sozialdaten. Voraussetzungen der angemessenen Nachvollziehbarkeit sind eine aussagefähige Protokollierung der Änderungen und Zugriffe auf personenbezogene Daten und geeignete Auswertungsmöglichkeiten für die Protokolldateien.

Im Zusammenhang mit dem Projekt oscare (vgl. Nr. 5.4.1) haben die Arbeitskreise Technik sowie Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gemeinsam „Empfehlungen zur Protokollierung in zentralen IT-Verfahren der Gesetzlichen Krankenversicherung“ erarbeitet. Der Leitfaden enthält Aussagen zu

- den rechtlichen Grundlagen,
- der Art und dem Umfang der Protokollierung sowie deren Nutzung und Auswertung,
- der Protokollierung von Daten aus der Verfahrensnutzung,
- der Protokollierung administrativer Zugriffe,
- der Zweckbindung sowie
- der Speicherungsdauer der Gesundheits- und Sozialdaten.

Die meiner Zuständigkeit unterliegenden Krankenkassen habe ich über die Orientierungshilfe informiert und um Beachtung der Empfehlungen bei den eingesetzten IT-Verfahren gebeten.

Auch wenn sich die Orientierungshilfe an die gesetzlichen Krankenkassen richtet, enthält sie auch wertvolle Hinweise, die für die Protokollierung bei IT-Verfahren in anderen Bereichen hilfreich sein können.

Abrufbar ist die Orientierungshilfe auf meiner Internetseite (www.datenschutz.bund.de) unter Informationsmaterial und Arbeitshilfen.

### 11.1.8 Anbindung medizinischer Subsysteme an ein Klinikinformationssystem

*Bei der geplanten Anbindung medizinisch-technischer Geräte mit sensiblen personenbezogenen Daten der Patienten an das Klinikinformationssystem der DRV Bund ist eine datenschutzgerechte Ausgestaltung von großer Bedeutung.*

Bei der Kontrolle einer Rehabilitationsklinik der DRV Bund im Jahre 2006 habe ich verschiedene medizinisch-technische Geräte geprüft, mit denen sensible medizinische Daten verarbeitet werden. Dabei hatte ich der DRV Bund Handlungsbedarf zum Schutz der auf diesen Geräten gespeicherten personenbezogenen Daten für alle ihre Rehabilitationszentren aufgezeigt und meine Beratung bei deren Konzeption angeboten (vgl. 21. TB Nr. 13.4.2). Daraufhin hat mir die DRV Bund mitgeteilt, dass sie an der Anbindung derartiger labor-/medizinisch-diagnostischer Subsysteme in ihren Rehabilitationszentren an das eigene Klinikinformationssystem KLInet arbeite.

Im Berichtszeitraum hat mir die DRV Bund nunmehr ihre Planungen zum Einsatz des Systems SUBsys II (Sonderverfahren bzw. -netze IT integrativer Bestandteil im Bereich Medizintechnik/Diagnostik u. ä.) vorgestellt. Hierzu habe ich konkrete datenschutzrechtliche Empfehlungen und Hinweise gegeben, die etwa die technisch-organisatorischen Regelungen oder die Erhebung, Verarbeitung oder

Nutzung von Sozialdaten im Auftrag nach § 80 SGB X (vgl. hierzu Nr. 11.1.2) betreffen.

Bei einem weiteren Beratungsbesuch, der den praktischen Einsatz des Systems SUBsys II in einem Reha-Zentrum zum Gegenstand hatte, galt mein besonderes Augenmerk den dortigen Möglichkeiten der Anbindung der unterschiedlichen medizinisch-technischen Geräte, mit denen Gesundheitsdaten der Patienten verarbeitet werden, an KLInet. Bei der Kontrolle habe ich die bestehenden vertraglichen Regelungen mit Dritten, die – soweit vorhanden – datenschutzrechtlichen Konzepte (etwa zur Sicherstellung der Auskunftsrechte der Betroffenen) sowie die technischen und organisatorischen Gegebenheiten im Praxisbetrieb des Reha-Zentrums näher einbezogen. Im Ergebnis habe ich erhebliche den Datenschutz betreffende Defizite festgestellt und umfassende Empfehlungen zu deren Behebung gegeben. Diese betrafen beispielsweise die vertraglichen Ausgestaltungen nach § 80 SGB X, die Dokumentationen zum Einsatz der im Reha-Zentrum in Augenschein genommenen klinikeigenen sowie der geleasten medizinisch-technischen Geräte sowie Datensicherheits- und Datenschutzkonzepte.

Der DRV Bund habe ich geraten, die Einbindung weiterer Subsysteme an KLInet erst dann umzusetzen, wenn die von mir empfohlenen Datenschutz- und Datensicherheitsmaßnahmen gewährleistet werden können. Die DRV Bund hat mich im Anschluss darüber unterrichtet, dass sie alle meine Empfehlungen aufgegriffen habe. Zudem werde sie bei den weiteren Planungen meine datenschutzrechtliche Beratung in Anspruch nehmen.

Ich werde im Rahmen meiner Beratungsaufgabe beim aktuellen und künftigen Einsatz medizinisch-technischer Geräte besonders darauf achten, dass beim beschriebenen Umgang mit diesen sensiblen personenbezogenen Daten die Persönlichkeitsrechte der Betroffenen gewahrt bleiben.

### 11.1.9 Kontrolle einer Leistungsabteilung der Deutschen Rentenversicherung Bund

*Ein Kontroll- und Beratungsbesuch in einer Leistungsabteilung der DRV Bund offenbarte erhebliche Schwachstellen. Die DRV Bund hat meine Anregungen weitgehend aufgegriffen.*

Gegenstand des Beratungs- und Kontrollbesuches in einer Leistungsabteilung der DRV Bund waren verschiedene Bereiche bzw. Dezernate. Dort habe ich schwerpunktmäßig den Umgang mit personenbezogenen Daten der Versicherten, u. a. durch eine stichprobenartige inhaltliche Prüfung von Versichertenakten, aber auch der Beschäftigten kontrolliert und hierzu datenschutzrechtliche Hinweise und Empfehlungen gegeben.

Der Austausch von Leistungsakten zwischen der Hauptstelle der DRV Bund und dieser Leistungsabteilung erfolgt täglich mit einem eigenen Lkw. Hierfür werden auf dem Transportwege mit einem Vorhängeschloss gesicherte Aktenwagen eingesetzt, in denen jeweils eine große Anzahl Akten und Vorgänge mit Sozialdaten transportiert werden. Bei der Zwischenlagerung der Aktenwagen nach der Anlieferung aus Berlin und vor einem Transport zur Hauptstelle habe ich festgestellt, dass ein Zugang zu den Sozialdaten für unbefugte Dritte sowie für unberechtigte Beschäftigte möglich war. Die DRV Bund hat umgehend reagiert und sofort nach dem Kontroll- und Beratungsbesuch die erforderlichen Maßnahmen getroffen. Dies habe ich ausdrücklich begrüßt.

Stichprobenartig habe ich auch Einsicht in Akten der Leistungsabteilung genommen und deren Inhalt auf Rechtmäßigkeit kontrolliert. Von mir in Einzelfällen aufgezeigter Handlungsbedarf, etwa zu in Leistungsakten aufgefundenen Kopien von Schul- oder Prüfungszeugnissen mit jeweils nicht geschwärzten Schul- bzw. Prüfnoten, hat umgehend zu ersten datenschutzgerechten Lösungen geführt. Zu anderen grundsätzlichen Themen stehe ich noch in Gesprächen mit der DRV Bund, ebenso zu einigen Feststellungen, die ich bei der Prüfung des Umgangs der Leistungsabteilung mit Beschäftigtendaten getroffen habe. Das grundsätzliche Problem der nach den Regelungen des BBG erforderlichen, bisher aber nicht erfolgten Löschungen von Abwesenheitszeiten (Personalaktendaten) im Personalwirtschaftsverfahren (Personalinformationssystem SAP R/3 HR) werde ich weiter mit hoher Priorität verfolgen. Näheres hierzu vgl. Nr. 5.4.2.

Unter Berücksichtigung der konstruktiven und zügigen Umsetzung der von mir vorgetragenen datenschutzrechtlichen Hinweise und Empfehlungen noch während oder unmittelbar im Anschluss an den Kontroll- und Beratungsbesuch konnte ich nach § 81 Absatz 2 SGB X i. V. m. § 25 Absatz 2 BDSG davon absehen, die festgestellten Verstöße gegenüber der DRV Bund förmlich zu beanstanden.

### 11.1.10 Ersatzkasse vermittelte psychisch Erkrankte zur Betreuung älterer Menschen

*Eine Ersatzkasse suchte ihren Versichertendatenbestand nach psychisch erkrankten Personen durch, die für die Teilnahme an einer ehrenamtlichen Maßnahme in Betracht kommen – ein äußerst bedenkliches Projekt.*

Durch eine Eingabe wurde ich darauf aufmerksam, dass in einer regionalen Geschäftsstelle einer Ersatzkasse ein datenschutzrechtlich äußerst bedenkliches Projekt durchgeführt wurde. Begrüßenswertes Ziel des Projektes war es, psychisch erkrankten Personen den Wiedereinstieg in ein geregeltes Leben zu erleichtern. Zu diesem Zweck kooperierte die Ersatzkasse mit dem Caritasverband, der dem betroffenen Personenkreis anbot, sich ehrenamtlich – z. B. durch die Betreuung älterer Menschen – zu engagieren. Zur Ermittlung der in Betracht kommenden Personen wertete die Ersatzkasse ihren Datenbestand nach Medikamentenverordnungen, Krankenhauseinweisungsdiagnosen etc. aus. Anschließend informierte sie die ermittelten psychisch erkrankten Personen über das Angebot des Caritasverbands. Die Kontaktaufnahme zum Caritasverband durch die angeworbenen Versicherten und die Teilnahme an der sozialen Maßnahme erfolgten auf freiwilliger Basis. Zur Abrechnung der vertraglich vereinbarten Vergütung informierte der Caritasverband die Ersatzkasse darüber, welche Versicherten an dem Projekt teilgenommen hatten.

Mangels einer gesetzlichen Grundlage oder einer Einwilligung der Betroffenen war die mit der Durchführung des Projektes einhergehende Auswertung der gespeicherten Versichertendaten und die anschließende Nutzung der Daten unzulässig. Zudem bestehen erhebliche Zweifel, ob die mit dem Caritasverband vertraglich vereinbarte Leistung überhaupt als eine solche angesehen werden kann, die von der Kasse im Rahmen ihrer gesetzlich zugewiesenen Aufgaben erbracht werden darf. Nachdem ich der Ersatzkasse meine datenschutzrechtlichen Bedenken mitgeteilt hatte, versicherte mir diese, die kritisierten Verträge seien nur regional begrenzt abgeschlossen worden und zwischenzeitlich ausgelaufen. Verlängert oder neu abgeschlossen würden entsprechende Verträge nicht.

## 11.2 Runder Tisch – Heimerziehung in den 50er und 60er Jahren

*Nach fast zweijähriger Arbeit hat der „Runde Tisch Heimerziehung in den 50er und 60er Jahren" im Dezember 2010 seinen Abschlussbericht vorgelegt. Meine datenschutzrechtlichen Anregungen wurden berücksichtigt.*

Der im Auftrag des Bundestages eingerichtete Runde Tisch sollte das Schicksal ehemaliger Heimkinder aufarbeiten, die in staatlichen, kirchlichen und privaten Heimen in Westdeutschland untergebracht und dort zum Teil schwer misshandelt worden waren. Der Appell des Runden Tisches an alle Einrichtungen und Institutionen, den ehemaligen Heimkindern Einsicht in die sie betreffenden Akten zu ermöglichen und zu erleichtern, wird von mir nachdrücklich unterstützt.

Nachdem sich eine Reihe ehemaliger Heimkinder im Frühjahr 2006 an den Petitionsausschuss des Deutschen Bundestages gewandt hatte, konstituierte der Bundestag mit einstimmigem Beschluss im Februar 2009 den „Runden Tisch Heimerziehung in den 50er und 60er Jahren". An dem von der ehemaligen Bundestagsvizepräsidentin Dr. Antje Vollmer moderierten Runden Tisch haben neben Vertretern des Petitionsausschusses des Deutschen Bundestages auch Vertreter der zuständigen Bundesministerien, der kirchlichen und staatlichen Träger der Heime sowie Vertreter ehemaliger Heimkinder teilgenommen.

Da für die persönliche Aufarbeitung die Kenntnis der Betroffenen über Familiengeschichte, Herkunft und die Entwicklung in der Kindheit unumgänglich ist, bestand das zentrale Anliegen der ehemaligen Heimkinder darin, Einsicht in ihre Heim- oder Krankenakten, aber auch in die Akten der Heimleitungen oder der Jugendämter, nehmen zu können oder zumindest Kenntnis über deren Inhalt zu erlangen.

Da sich die Heime in unterschiedlicher Trägerschaft und in verschiedenen Bundesländern. befunden haben, sind die für die Akteneinsicht bzw. Auskunftserteilung anzuwendenden Rechtsvorschriften zwar unterschiedlich. Im Wesentlichen orientieren sich die Rechte der Betroffenen aber an den Regelungen des Zehnten Sozialgesetzbuches (SGB X). Danach ist sowohl das Akteneinsichtsrecht der Betroffenen nach § 25 SGB X als auch das Auskunftsrecht nach § 83 SGB X eingeschränkt, wenn Interessen Dritter entgegenstehen. Bei der Abwägung datenschutzrechtlicher Belange Dritter ist aber zu beachten, dass ehemalige Erzieher oder Angestellte von Kinderheimen, deren Name in Ausübung ihrer Funktion in die Akte aufgenommen wurde, im Gegensatz zu den ebenfalls in den Akten erwähnten anderen Heimkindern, grundsätzlich keinen Anspruch darauf haben, dass ihre Namen unkenntlich gemacht werden. Das Interesse der Funktionsträger an der Geheimhaltung ihrer Namen tritt vielmehr hinter das Informationsinteresse der Betroffenen zurück. Die Namen anderer Heimkinder müssen hingegen vor Gewährung der Akteineinsicht unkenntlich gemacht werden.

Auch der Umstand, dass bei vielen Akten angesichts der verstrichenen Zeit bereits die Aufbewahrungsfrist abgelaufen ist, steht dem Recht auf Akteneinsicht und Auskunft der ehemaligen Heimkinder nicht entgegen. Altakten, deren Aufbewahrungsfrist verstrichen ist, dürfen nämlich nicht einfach vernichtet werden. Dies ergibt sich aus dem Rechtsgedanken des § 84 Absatz 2 Satz 2 SGB X, wonach eine Löschung nur erfolgen darf, wenn kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Gerade dies wäre aber bei der Vernichtung der Akten der Fall, da das schützenswerte Interesse der Betroffenen auf Auskunft und Erhalt ihrer Unterlagen unwiederbringlich vereitelt würde.

Neben der Hilfestellung bei der persönlichen Bewältigung des Erlebten durch die Betroffenen hatte der Petitionsausschuss bereits bei Einrichtung des Runden Tisches empfohlen, die Geschehnisse in der Heimerziehung im westlichen Nachkriegs-Deutschland unter den damaligen rechtlichen, pädagogischen und sozialen Bedingungen auch wissenschaftlich aufzuarbeiten. Für die Übermittlung der personenbezogenen Daten für wissenschaftliche Zwecke wird in der Regel allerdings die Einwilligung der Betroffenen erforderlich sein. Dies folgt aus dem besonderen Schutz der Sozialdaten und des Sozialgeheimnisses. Jugendämter und öffentlich-rechtliche Träger unterliegen insofern den Einschränkungen des § 75 SGB X, wenn sie Sozialdaten für die Forschung übermitteln wollen. Für freie und kirchliche Träger gelten teilweise abweichende Bestimmungen, sodass in diesen Fällen eine Prüfung des Einzelfalls erfolgen muss. Aber auch hier ist es geboten, dass eine wissenschaftliche Aufarbeitung nur unter strikter Beachtung des informationellen Selbstbestimmungsrechts der Betroffenen erfolgt.

Ich habe den Runden Tisch auf dessen Bitte hin bei datenschutzrechtlichen Fragen unterstützt. Er hat meine Anregungen aufgegriffen.

## 11.3 Kontrolle des Paul-Ehrlich-Instituts offenbarte Datenschutzverstöße

*Im Rahmen eines Beratungs- und Kontrollbesuchs beim Paul-Ehrlich-Institut habe ich mich insbesondere mit der datenschutzgerechten Ausgestaltung des Forschungsprojekts „Humanes endogenes Retrovirus, Typ K (HERV-K)" sowie des Deutschen Hämophilieregisters beschäftigt.*

Das Paul-Ehrlich-Institut (PEI) befasst sich im Wesentlichen mit der Zulassung biomedizinischer Produkte und Impfstoffe, Maßnahmen im Bereich der Risikovorsorge und im Zusammenhang mit Humanarzneimitteln sowie mit hierauf bezogenen Forschungsprojekten.

**Forschungsprojekt „Humanes endogenes Retrovirus, Typ K (HERV-K)“**

Die Erforschung humaner endogener Retroviren des Typs K (dazu gehört HERV-K) ist einer der Arbeitsschwerpunkte des PEI. Ziel ist es, die Behandlung bei Tumor-, Autoimmun- und HIV-Erkrankungen zu verbessern.

Das Erheben, Speichern, Verändern und Nutzen personenbezogener Daten in der entsprechenden Projektdatenbank ist zulässig, da dies zur Erfüllung der in der Zuständigkeit des PEI liegenden Aufgaben (hier: Forschung) erforderlich ist. Dem steht nicht entgegen, dass bisherige Zwischenergebnisse den vermuteten Zusammenhang zwischen dem Virus HERV-K und dem Entstehen einer HIV-Infektion nicht aufzeigen. Denn es liegt in der Natur der Sache, dass bei komplexen medizinischen Forschungen mit raschen Ergebnissen nicht gerechnet werden kann. Damit ist die Datenerhebung selbst zwar rechtmäßig, die Art und Weise der Datenspeicherung und -nutzung jedoch problematisch:

Die Speicherung der Datensätze mit Angaben zum Gesundheitszustand bzw. Diagnosen erfolgte ohne Einwilligung der Betroffenen und teilweise unter Nennung der Klarnamen. Dies betraf auch die Referenzdaten, die von Mitarbeitern des PEI erhoben wurden, wobei hier zumindest eine mündliche Einwilligung der Betroffenen gegeben wurde. Die Datei wurde unverschlüsselt geführt; die Zugangsberechtigungen waren nicht geregelt.

Inzwischen hat das PEI die festgestellten Mängel beseitigt: Der Personenbezug bei den bestehenden Daten wurde gelöscht, neue Datensätze werden nur noch in anonymisierter Form gespeichert. Zusätzlich wird die Datenbank mittels der Verschlüsselungssoftware „True Crypt“ verschlüsselt.

**Das Deutsche Hämophilieregister**

Nach dem Transfusionsgesetz (TFG) hat das PEI die Aufgabe, die Anzahl behandlungsbedürftiger Hämophiliepatienten und den Versorgungsgrad mit Blutprodukten auszuwerten. Hierfür betreibt das PEI das Deutsche Hämophilieregister (DHR) auf der Basis eines zusammen mit der Gesellschaft für Thrombose- und Hämostaseforschung, der Deutschen Hämophiliegesellschaft zur Bekämpfung von Blutungskrankheiten und der Interessengemeinschaft Hämophiler erarbeiteten Konzepts. Außerdem wird mit Hilfe der im DHR gespeicherten Krankheits- und Therapiedaten diese seltene Krankheit mit dem Ziel erforscht, die Behandlung Betroffener zu verbessern und dabei die Behandlungskosten zu senken. Für die Umsetzung der technisch–organisatorischen Einrichtung des Registers mussten die unterschiedlichen Anforderungen seitens der Ärzte und Patienten, der Wissenschaftler und des PEI berücksichtigt werden. Niedergelassene Ärzte und Krankenhäuser stellen nach Autorisierung mittels eines Benutzernamens und einer Ident-Nummer die umfangreichen Daten ihrer Hämophiliepatienten (Patientennummer, Geburtsmonat, Geburtsjahr, Geschlecht, zwei Ziffern seiner Postleitzahl, diagnostische und therapeutische Daten sowie behandlungsbezogene Qualitätssicherungs-Daten) selbst in das DHR ein. Dabei wird die Patientennummer zunächst auf einem Rechner ohne Festplatte pseudonymisiert, bevor der Datensatz in das DHR überführt wird. Betreiber des festplattenlosen Rechners ist die Stadt Langen, mit der das PEI einen entsprechenden Kooperationsvertrag geschlossen hat.

Für die beschriebene Forschungsnutzung werden die pseudonymisierten Daten durch Löschen des Pseudonyms mit Ausnahme der Behandlungsdaten, des Geburtsjahrs und der ersten beiden Ziffern der Postleitzahl des Patienten anonymisiert. Jeder Behandler kann nur auf die von ihm selbst eingestellten Daten zugreifen; ein Zugriff auf die gesamte Behandlungshistorie eines Patienten, der bei unterschiedlichen Ärzten bzw. Krankenhäusern in Behandlung war, ist nicht möglich. Die beschriebene Konzeption für den Betrieb des DHR wirft einige datenschutzrechtliche Fragen auf.

– Pseudonymisierung

  Personenbezogene Forschungsdaten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert. Die im DHR erfassten Daten sind demnach spätestens nach Abschluss der Erhebung zu anonymisieren, sofern es keiner Ergänzungen bei fortgeführter (in der Regel lebenslanger) Hämophilietherapie oder keiner Kontrollen mehr bedarf.

  Die Speicherung der Patientendaten im DHR erfolgt unter einem Pseudonym. Für dessen Berechnung im festplattenlosen Rechner wird die Patientennummer verwendet, die sich aus der Krankenversichertennummer und dem Institutionskennzeichen der Krankenkasse des Patienten zusammensetzt. Neben dem pseudonymisierten Patientendatensatz werden auch Arztdaten (Praxisdaten des Behandlers wie etwa Name, Anschrift und Telefonnummer) gespeichert. Damit könnte das Pseudonym – allerdings mit erhöhtem Aufwand – reidentifiziert werden. Um dies zu vermeiden, habe ich eine Pseudonymisierung der Arztdaten gefordert. Die Umsetzung dieser Forderung durch das PEI werde ich beratend begleiten.

– Auskunftsrecht der Patienten

  Die Patienten haben jederzeit das Recht, Auskunft bezüglich der im DHR über sie gespeicherten Daten zu erhalten. Die Datenbank des PEI lässt einen hierfür erforderlichen Zugriff auf alle Patientendaten jedoch nicht zu. Eine Änderung wollte das PEI zunächst nicht vornehmen, da die Patientendaten nach § 14 Absatz 3 TFG für die Dauer von 15 Jahren bereits von anderen Stellen vorgehalten werden müssen. Daher sei es nach

seiner Ansicht dem Patienten zumutbar, sein Auskunftsrecht diesen Stellen gegenüber auszuüben. Dies sind

- sein niedergelassener Arzt,
- sofern der Arzt seine Praxis ohne Nachfolger aufgegeben hat oder verstorben ist, die zuständige Kassenärztliche Vereinigung
- und/oder das ihn behandelnde Krankenhaus.

Die Auffassung des PEI, es ergebe sich weder aus dem BDSG noch aus dem TFG eine Verpflichtung, das Auskunftsrecht für den Betroffenen so einfach wie möglich zu gestalten, habe ich nicht geteilt.

Da das PEI sich jedoch entschlossen hat, meiner Forderung nach einer Pseudonymisierung der Arztdaten zu folgen, ist auch dieses Problem gelöst, so dass Patienten künftig für eine Dauer von zwei Jahren auf alle über sie gespeicherten Daten zugreifen können. Danach erlischt das Recht auf Auskunftserteilung, da die Daten tatsächlich nicht mehr personenbezogen gespeichert sind.

- Anonymisierung der Patientendaten

  Die Patientendaten werden mit Ausnahme der Behandlungsdaten, des Geburtsjahrs und der ersten beiden Ziffern der Postleitzahl der Patienten durch die Löschung des Pseudonyms anonymisiert. Bei geringer Bevölkerungsdichte (unter 250 000 Einwohner pro Postleitzahlregion) liegt jedoch keine Anonymisierung nach § 3 Absatz 6 BDSG vor, weil nicht zuletzt aufgrund der Seltenheit des Krankheitsbildes in Verbindung mit den anonymisierten und den pseudonymisiert bleibenden Patientendaten die Herstellung des Personenbezugs ohne unverhältnismäßigen Zeit-, Kosten- und Kraftaufwand möglich wäre. Die Einspeisung der Daten aus der einzigen unter dem Schwellenwert von 250 000 Einwohnern liegenden Postleitzahlregion in das DHR erfolgt daher künftig zusammen mit der Einspeisung der Daten aus einer zweiten Postleitzahlregion. Mit der hiermit erreichten Überschreitung des Schwellenwertes von 250 000 Einwohnern sind die Daten ausreichend anonymisiert. Damit wurde meinen Bedenken Rechnung getragen.

## 11.4 Forschungsprojekt des Robert-Koch-Instituts zum Thema Schweinegrippe

*Angesichts des befürchteten Ausbruchs einer Schweinegrippenpandemie hatte das Robert-Koch-Institut (RKI) in Berlin eine krankenhausbasierte Fall-Kontrollstudie zur Wirksamkeit von Schweinegrippenimpfstoffen geplant.*

Im Vorfeld der Studie hat mich das RKI um datenschutzrechtliche Beratung bezüglich der vorgesehenen Verarbeitung personenbezogener Daten von Schweinegrippe-Patienten sowie hieran nicht erkrankter Patienten aus Krankenhäusern in Berlin gebeten.

Soweit für die Studie außerdem Daten von Versicherten der AOK Berlin und durch Melderegisterauskunft bei der Berliner Verwaltung gewonnener Teilnehmer einbezogen werden sollten, hat der Berliner Landesdatenschutzbeauftragte den Beratungsprozess unterstützt.

Die datenschutzrechtlichen Fragestellungen ähnelten den Aspekten, die auch bei meiner Beratung des Bundesinstituts für Sportwissenschaft bei dessen Dopingforschungsprojekt eine Rolle spielten (vgl. Nr. 8.7).

Das RKI ist meinen Empfehlungen gefolgt, die Einwilligungserklärung sowie ein Informationsschreiben an die zur Teilnahme vorgesehenen Personen zu präzisieren. Ich habe darum gebeten, die Hinweise auf das uneingeschränkte Auskunftsrecht der Betroffenen zu verbessern. Außerdem habe ich Ratschläge zur schriftlichen Dokumentation der auf Einwilligung der Betroffenen beruhenden Datenerhebungen bei deren Hausärzten für die Fälle erteilt, in denen die Einwilligung durch die Forscherinnen und Forscher telefonisch eingeholt wird.

## 11.5 Arbeitsverwaltung

### 11.5.1 Aufsichtszuständigkeit über die neu geschaffenen Jobcenter

*Seit dem 1. Januar 2011 unterliegen die bislang von den Landesbeauftragten kontrollierten Mischbehörden ausschließlich meiner Zuständigkeit. Dem daraus resultierenden zusätzlichen Personalbedarf in meiner Dienststelle wurde noch nicht nachhaltig Rechnung getragen.*

Mit dem am 1. Januar 2011 in Kraft getretenen „Gesetz zur Weiterentwicklung der Organisation der Grundsicherung für Arbeitsuchende“ (BGBl. I 2010 S. 1112) wird in § 50 Absatz 4 SGB II geregelt, dass die Datenschutzkontrolle und die Kontrolle der Einhaltung der Vorschriften über die Informationsfreiheit bei der gemeinsamen Einrichtung sowie für die zentralen Verfahren der Informationstechnik nach § 24 BDSG dem BfDI obliegen.

Die bisher gemeinsam von der Bundesagentur für Arbeit (BA) und den Kommunen in den 346 sog. Arbeitsgemeinschaften (ARGE) wahrgenommenen Aufgaben werden nach der Neuregelung auch weiterhin in „Gemeinsamen Einrichtungen“ (neu: Jobcentern) durchgeführt. Dabei sind die BA und die Kommunen weiterhin Leistungsträger im Sinne des SGB und die Jobcenter verantwortliche Stellen. Dies entspricht im Wesentlichen der bisherigen Regelung.

Bis zur Neuregelung unterlagen die ARGE als Stellen der Länder der Kontrolle der Landesbeauftragten für den Datenschutz (§ 81 Absatz 1 Nr. 2, Absatz 3 SGB X). Lediglich soweit die BA zentrale EDV-Programme den ARGE zur Verfügung gestellt oder generelle Vorgaben getroffen hat, war meine Zuständigkeit begründet.

Diese Aufgabenteilung mit meinen Länderkolleginnen und -kollegen hatte sich aus meiner Sicht bewährt und gewährleistete eine effiziente und bürgernahe Datenschutzkontrolle „vor Ort“. Durch den Verzicht auf diese sachgerechte Differenzierung wurde der Vorteil der räumlichen Nähe zur beaufsichtigten Stelle preisgegeben. Ich hatte mich daher gegen diese Änderung der Zuständigkeitsregel ausgesprochen.

Von entscheidender Bedeutung ist künftig, im Interesse der Betroffenen auch weiterhin eine effiziente Daten-

schutzaufsicht zu gewährleisten. Dies ist nur mit einer entsprechenden personellen Ausstattung meiner Behörde zu leisten. Die insoweit zur Aufgabenerledigung notwendigen 15 Planstellen sind mir im Haushalt 2011 nicht gewährt worden. Es wurden lediglich entsprechende Finanzmittel für die Personalausgaben eingestellt, was zunächst nur befristete Arbeitsverhältnisse zulässt. Dies ist allenfalls für eine Übergangszeit vertretbar. Um meinen gesetzlichen Auftrag erfüllen zu können, sind möglichst bald Planstellen für diese dauerhafte Aufgabe zu schaffen.

### 11.5.2 Reform von „Hartz IV“ – Bildungsgutscheine und Datenschutz

*Die vom Bundesverfassungsgericht (BVerfG) ausgelöste Neubemessung des Regelbedarfs hat auch eine datenschutzrechtliche Komponente. Meinen diesbezüglichen Forderungen wurde im wesentlichen Rechnung getragen.*

Mit dem Urteil des BVerfG vom 9. Februar 2010 (1 BvL 1/09, 1 BvL 3/09, 1 BvL 4/09) wurde dem Gesetzgeber aufgegeben, die Regelbedarfe nach SGB II und SGB XII verfassungskonform neu zu bemessen. Einen besonderen Stellenwert räumt das Gericht dabei dem Bedarf von Kindern und Jugendlichen ein, für deren größere soziale Integration und bessere Chancen auf Bildung und Teilhabe künftig besondere Leistungen – wie etwa für Lernförderung, Mittagsverpflegung und Klassenfahrten oder für die Teilnahme am sozialen und kulturellen Leben – vorzusehen sind.

Der Entwurf eines Gesetzes zur Ermittlung von Regelbedarfen und zur Änderung des Zweiten und Zwölften Buches Sozialgesetzbuch sah für die Erbringung dieser Leistungen zunächst die Ausgabe von personalisierten Gutscheinen vor, während eine anonyme Form von Kostenübernahmeerklärungen gegenüber leistungsberechtigten Personen auf bestimmte Sachverhalte beschränkt war. Zudem sollte das Bundesministerium für Arbeit und Soziales (BMAS) pauschal ermächtigt werden, durch Rechtsverordnung die Entwicklung, das Verfahren und die Nutzung eines elektronischen Abrechnungssystems zur Leistungserbringung sowie zur Einlösung und Abrechnung der Gutscheine zu regeln.

Im Rahmen meiner Beteiligung habe ich mit Blick auf die personalisierten Gutscheine auf das verfassungsrechtliche Risiko einer Offenbarungspflicht Hilfebedürftiger gegenüber Dritten hingewiesen, deren „Verortung“ als hilfebedürftig ihrem Grundrecht auf informationelle Selbstbestimmung zuwiderliefe. Stattdessen schlug ich vor, für alle Leistungen für Bildung und Teilhabe als Alternative zu personalisierten Gutscheinen die direkte Zahlung an die Anbieter dieser Leistungen vorzusehen. Dem entspricht die aktuelle Fassung der §§ 29 bis 30a SGB II-Entwurf und § 34a SGB XII-Entwurf.

Auch bei der Ausgestaltung der Verordnungsermächtigung zum geplanten elektronischen Abrechnungssystem für die Leistungserbringung sowie zur Einlösung und Abrechnung von Gutscheinen („Bildungschipkarte“) ist mir das BMAS entgegengekommen.

Ich hatte erhebliche Zweifel, ob die Festlegung der Grundzüge wie der Einzelheiten eines solchen Verfahrens dem Verordnungsgeber überlassen werden darf. Denn der Normgeber ist verpflichtet, im Bereich der Grundrechtsausübung alle wesentlichen Entscheidungen selbst zu treffen. Je intensiver ein Sachverhalt die Grundrechte berührt, desto eher muss dieser gesetzlich geregelt werden. Dies gilt vor allem bei technischen Neuerungen, wobei die Einrichtung elektronischer Abrechnungssysteme und der Einsatz der Chipkartentechnik klassische Beispiele für die Notwendigkeit gesetzlicher Regelungen zur Eingrenzung technisch bewirkter Grundrechtsrisiken bilden.

Für den Fall, dass es gleichwohl bei einer Regelung durch Rechtsverordnung bleiben solle, wies ich das BMAS darauf hin, dass eine lediglich pauschale Verordnungsermächtigung – wie ursprünglich vorgesehen – keinesfalls ausreichend sei. Im Rahmen der näheren Darlegung von Inhalt, Zweck und Ausmaß der beabsichtigten Verordnung müsse die Ermächtigungsnorm grundrechtswahrend detaillierte Vorgaben mit Blick auf das informationelle Selbstbestimmungsrecht enthalten.

Nunmehr sieht der überarbeitete Entwurf einer Verordnungsermächtigung in § 29 Absatz 3 SGB II vor, dass das BMAS durch Rechtsverordnung auch das Nähere über die Erhebung, Verarbeitung und Nutzung der Sozialdaten bestimmt, die für den Zweck der Erbringung und Abrechnung von Leistungen mittels eines elektronischen Systems erforderlich sind. In der Rechtsverordnung ist jetzt auch das Nähere zur Datensicherheit, insbesondere durch technische Absicherungen im System, zu bestimmen. Damit wird auch in dieser Frage meinen Anregungen Rechnung getragen.

Das Gesetzgebungsverfahren ist noch nicht abgeschlossen.

### 11.5.3 E-Akte der Bundesagentur für Arbeit

*Die Bundesagentur für Arbeit will ihre Papier-Kundenakten auf elektronische Akten (E-Akte) umstellen. Die Digitalisierung des Schriftguts soll durch einen Privatdienstleister erfolgen. Dagegen bestehen keine grundlegenden Datenschutzbedenken.*

Die BA will zukünftig ihre Papierakten vollständig durch elektronische Akten ersetzen. Die Umstellung soll als Pilotprojekt in Sachsen-Anhalt und Thüringen starten, zunächst für die Arbeitslosenversicherung („Arbeitslosengeld I“) und in der Familienkasse („Kindergeld“). Insgesamt liegen nach Angaben der Bundesagentur über 35 Millionen Kundenakten vor, täglich gehen 400 000 neue Dokumente ein. Kundenakten und eingehende Briefe sollen in einem Scan-Zentrum der Deutschen Post AG digitalisiert werden, die von der BA dazu beauftragt worden ist.

Dass auch ein Sozialleistungsträger wie die BA sich eines privaten Dienstleisters zur Erhebung, Verarbeitung oder Nutzung von Sozialdaten bedienen will, ist nur unter den engen Voraussetzungen des § 80 Absatz 5 SGB X (z. B. bei Störungen im Betriebsablauf oder bei erheblich kostengünstigerer Besorgung durch den Dienstleister) zulässig.

Entscheidend kommt es bei einem Projekt dieser Größenordnung darauf an, ob die BA als Auftraggeberin wegen der besonderen Schutzbedürftigkeit der Sozialdaten der Arbeitsuchenden höchste Anforderungen an die technischen und organisatorischen Maßnahmen stellt, die der Auftragnehmer zu treffen hat.

Maßstab ist insoweit die zur Auftragsdatenverarbeitung von Sozialdaten am 11. August 2010 in Kraft getretene Spezialnorm des § 80 SGB X (vgl. Nr. 11.1.2). Diese Vorschrift gilt auch für Altverträge, die entsprechend anzupassen sind.

Ich habe den Vertrag der BA mit der Deutschen Post AG vom 13. Mai/29. Mai 2009 hierauf überprüft und keine gravierenden Mängel festgestellt. Zu wenigen Einzelpunkten bin ich noch im Gespräch mit der BA.

Ein digitaler Posteingangsservice wird bereits seit einigen Jahren von der Deutschen Post AG angeboten. Auch wenn das insoweit tätige Tochterunternehmen nicht meiner datenschutzrechtlichen Kontrollbefugnis unterliegt – zuständig wäre hier die Aufsichtsbehörde des Landes Baden-Württemberg –, hatte ich bei einem Informationsbesuch im Juni 2007 den Eindruck gewonnen, dass im Zusammenhang mit der Verarbeitung und Speicherung personenbezogener Daten datenschutzrechtliche Vorgaben eingehalten wurden. Seither sind mir keine Anhaltspunkte bekannt geworden, dass das Unternehmen gegen Datenschutzbestimmungen verstößt.

Wer seine Briefe dennoch nicht durch das Scan-Zentrum öffnen lassen will, hat alternativ die Möglichkeit, die Briefe weiterhin an die BA-Hausanschrift und nicht an die spezielle Großempfängerpostleitzahl zu adressieren. Die Öffnung, Sichtung und Steuerung des Schriftgutes soll nach Mitteilung der Bundesagentur in diesen Fällen weiterhin durch ihre Mitarbeiter erfolgen.

Ich werde das beabsichtigte Verfahren weiterhin kritisch begleiten und einer Überprüfung vor Ort unterziehen.

### 11.5.4 Einzelfälle

– Information über Arbeitslosigkeit eines Kunden der Agentur für Arbeit an eine Krankenversicherung ohne dessen Zustimmung

  Ein freiwillig weiterversicherter Petent wies mich darauf hin, dass er im Rahmen seiner Arbeitslosenmeldung bei der Agentur für Arbeit auch einen Nachweis über seine private Kranken- und Pflegeversicherung erbracht hatte. Die Agentur für Arbeit informierte daraufhin die Versicherung über die Arbeitslosigkeit des Petenten, was diese dem Betroffenen mitteilte.

  Hierin liegt ein Datenschutzverstoß, denn die Agentur für Arbeit hätte die Angaben zur Arbeitslosigkeit des Petenten an die Versicherung nur mit dessen Einwilligung weitergeben dürfen. Zwar lag eine solche Erklärung noch aus einem früheren Leistungsbezug vor, die Einwilligung des Petenten hätte aber aktuell eingeholt werden müssen. Dass dies nicht geschah, werte ich als Verstoß gegen § 4a BDSG.

  Ich habe die BA gebeten, die Agenturen für Arbeit darauf hinzuweisen, dass ohne eine aktuelle Einwilligung des Leistungsbeziehers Angaben zur Arbeitslosigkeit an Versicherungen nicht mitgeteilt werden dürfen.

  Da die BA den Verstoß einräumt und meine Hinweise künftig berücksichtigen will, habe ich von einer Beanstandung gemäß § 25 BDSG abgesehen.

– Übermittlung von Sozialdaten durch die BA an potentielle Arbeitgeber

  Mehrere Petenten, die ihr Bewerberprofil zur Stellensuche auf der Internet-Plattform der BA anonym veröffentlicht hatten, beschwerten sich darüber, dass sie Anrufe von Zeitarbeitsfirmen erhielten, die Einblick in das Bewerberprofil der Petenten hätten. Auf Nachfrage der Betroffenen, wie die Firmen an deren Kontaktdaten gelangen konnten, gaben die Agenturen für Arbeit an, einige Firmen hätten Zugang zu den gleichen personenbezogenen Daten wie die Arbeitsagentur selbst. Die Petenten hatten aber in die Weitergabe ihrer Daten nicht eingewilligt.

  Für die Übermittlung der freiwilligen Angaben wie Telefonnummer und E-Mail-Adresse sehe ich keine Rechtsgrundlage. Die BA hat auf meine Kritik hin zugesagt, die Übermittlung von Daten an potentielle Arbeitgeber im Rahmen der Vermittlung umzustellen.

  Bisher wurden bei der Buchung eines Vermittlungsvorschlages im Vermittlungsprogramm VerBIS bei gemeinsamer Nutzung des Jobbörsen-Accounts unabhängig vom Veröffentlichungsstatus des Bewerberangebots die Kontaktdaten des Kunden offenbart, weil dies im Zusammenhang mit der Vermittlung i. S. v. § 35 SGB III für erforderlich erachtet wurde.

  Dies wird die BA nun ändern und diese Kontaktdaten nur bei einer entsprechenden Einwilligung des Kunden für eine externe Veröffentlichung übermitteln. Es wird beim Kunden explizit abgefragt, ob er mit der externen Kommunikation einverstanden ist. Das Ergebnis soll in einem gesonderten Vermerk dokumentiert werden. Diese Einwilligungserklärung wird durch Mitarbeiter der BA in der Eingangszone oder im Servicecenter generiert, die Eingabe wird protokolliert und wäre auch innerhalb von 90 Tagen im Falle von Beschwerden überprüfbar.

  Stimmt der Kunde nicht zu, sind auch im Vermittlungsprozess Kontaktdaten wie Telefonnummer und E-Mail-Adresse nicht einsehbar und können mithin nicht mehr ausgedruckt werden.

  Die Vordrucke Vermittlungsvorschlag, die Leitfäden für die Servicecenter, Arbeitspakete etc. sollen nach Angaben der BA entsprechend angepasst werden.

– Vordruck „Entbindung von der Schweigepflicht gegenüber dem Psychologischen Dienst der Agentur für Arbeit“

  Ein Zentrum für Psychiatrie hat mir mitgeteilt, dass Agenturen für Arbeit dort umfangreiche medizinische

Daten von behandelten Patienten anfordern. Hierfür sollten sich Patienten damit einverstanden erklären, dass Befundunterlagen und Untersuchungsergebnisse sowie die Krankengeschichte der letzten fünf Kalenderjahre dem Psychologischen Dienst der Agentur für Arbeit zur Verfügung gestellt werden. Ich habe die BA gebeten, soweit möglich die angeforderten Daten konkret in die Schweigerpflichtentbindungs-Erklärung aufzunehmen sowie auf die Möglichkeit hinzuweisen, die Erklärung für die Zukunft zu widerrufen.

Wie die BA mir nun mitgeteilt hat, haben die Mitarbeiter des Psychologischen Dienstes der Agenturen für Arbeit zur Verwendung des Vordrucks entsprechende Bearbeitungshinweise erhalten. Neben den obligatorischen Inhalten – wer (Name, Anschrift, Geburtsdatum des Kunden) entbindet wen (namentlich zu benennender Arzt/Behandler) in Bezug auf was (zu übermittelnde Daten möglichst konkret) wofür (Zweck der Übermittlung) an wen (Empfänger namentlich) wie lange (einmalig oder wiederkehrend/zumindest datierte Erklärung) mit der Möglichkeit des Widerrufs – sind nunmehr der Kontext des Anliegens, die Erkrankung/Einschränkung, auf die sich der Klärungsbedarf bezieht sowie der aus fachlicher Sicht notwendige Betrachtungszeitraum in die Erklärung mit aufzunehmen. Die Vordrucke wurden entsprechend überarbeitet.

## 12 Mitarbeiterdatenschutz

### 12.1 Beschäftigtendatenschutz – wird endlich gut, was lange währt?

*Die Bundesregierung hat im Sommer 2010 den Entwurf eines Beschäftigtendatenschutzgesetzes vorgelegt, der den erst ein Jahr zuvor in Kraft getretenen § 32 BDSG ersetzen soll. Allerdings sehe ich noch in wichtigen Punkten erheblichen Verbesserungsbedarf.*

Offensichtlich bedurfte es erst spektakulärer Datenschutzskandale (vgl. u. Nr. 12.2), um den jahrzehntelangen Bemühungen um eine gesetzliche Regelung des Beschäftigtendatenschutzes neuen Schwung zu geben.

Im Jahr 2009 sah sich die Bundesregierung zu ersten Aktivitäten mit dem Ziel der gesetzlichen Verankerung datenschutzrechtlicher Regelungen im Arbeitsverhältnis veranlasst. Am 16. Februar 2009 beschäftigte sich eine Diskussionsrunde auf Einladung des Bundesinnenministers mit den notwendigen Verbesserungen des Datenschutzes für Arbeitnehmer und andere Beschäftigte. Die Sozialpartner nahmen an der Besprechung teil, zu der auch ich eingeladen war. Im Anschluss daran sagte die Bundesregierung die Schaffung einer Grundsatzregelung zur Stärkung des Arbeitnehmerdatenschutzes im Bundesdatenschutzgesetz zu, die von einer interministeriellen Arbeitsgruppe unter meiner Beteiligung vorbereitet werden sollte.

Parallel dazu zog der Gesetzgeber erste Konsequenzen aus den Datenschutzskandalen, indem er im Rahmen der BDSG-Novelle II (vgl. Nr. 2.2) mit § 32 BDSG neben einer „Grundsatzregelung“ zum Beschäftigtendatenschutz auch Vorgaben zum Abgleich von Beschäftigtendaten mit anderen Daten zu Strafverfolgungszwecken beschloss. Damit wurde zwar erstmals gesetzlich festgelegt, dass persönliche Daten, die für Beschäftigungsverhältnisse erhoben werden, grundsätzlich zu keinem anderen Zweck verwendet werden dürfen – viele weitere Fragen zum Umgang mit persönlichen Daten vor, während und nach Beendigung von Beschäftigungsverhältnissen blieben aber noch unbeantwortet.

Kurz vor der Bundestagswahl 2009 veröffentlichte das Bundesministerium für Arbeit und Soziales (BMAS) den Entwurf eines Beschäftigtendatenschutzgesetzes, den die SPD-Fraktion nach der Bundestagswahl unverändert in den Deutschen Bundestag einbrachte (Bundestagsdrucksache 17/69). Dieser Entwurf sieht ein eigenständiges Beschäftigtendatenschutzgesetz vor. Demgegenüber beschlossen die Regierungsparteien in der Koalitionsvereinbarung vom 26. Oktober 2009, den Arbeitnehmerdatenschutz in das Bundesdatenschutzgesetz zu integrieren.

Der Ende März 2010 vom Bundesministerium des Innern (BMI) übersandte Referentenentwurf setzte wesentliche Ziele zur Verbesserung des verfassungsrechtlich geschützten Persönlichkeitsrechts der Beschäftigten allerdings nicht um. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher in der Entschließung vom 22. Juni 2010 (vgl. Kasten zu Nr. 12.1) deutliche Kritik geäußert.

Im Zuge der folgenden Diskussionen und im Rahmen der Ressortabstimmungen konnten bereits einige datenschutzrechtliche Verbesserungen erreicht werden, die in den von der Bundesregierung am 25. August 2010 beschlossenen Gesetzentwurf Eingang fanden. Verbessert wurden beispielsweise die Regeln zu heimlichen Ermittlungsmaßnahmen, zur Videoüberwachungen und zu Datenabgleichen. Ich bewerte es positiv, dass heimliche Maßnahmen bei Datenabgleichverfahren („Datenscreening“) nur als ultima ratio zulässig sein sollen. Heimliche Ermittlungsmaßnahmen dürfen nur durchgeführt werden, wenn Tatsachen einen entsprechenden Verdacht stützen. Auch konnte erreicht werden, dass die erste Stufe bei Datenabgleichverfahren nur anonymisiert oder pseudonymisiert durchgeführt werden darf. Ebenso soll die heimliche Video-Überwachung unzulässig sein.

Neben diesen positiven Elementen sehe ich aber noch weiteren Verbesserungsbedarf:

- Datenabgleichverfahren sollten generell nur zulässig sein, wenn ein konkreter Anlass vorliegt. Routinemäßige Datenabgleiche zur Verdachtsgewinnung hielte ich für unverhältnismäßig.
- Die grundlegende Regelung zur heimlichen Datenverarbeitung sieht auch den Zweck der „Verhinderung weiterer Straftaten“ vor. Ich kann nicht nachvollziehen, in welchen Fallkonstellationen diese Regelung greifen soll, da sich solche Maßnahmen nur gegen Beschäftigte richten sollen, die bereits einer Straftat überführt worden sind und deshalb wohl kaum noch in dem Betrieb tätig sein dürften.

- Problematisch ist auch die vorgesehene sehr weitgehende Zulassung der Verwendung von Beschäftigtendaten zur Verhaltens- und Leistungskontrolle. So wurde in § 32i Absatz 3 BDSG-E, der vornehmlich E-Mail-Daten betrifft, eine entsprechende Formulierung aufgenommen. Auch dies halte ich für zu weitgehend.

- Die vorgesehene Erlaubnis zur offenen Videoüberwachung ist ebenfalls viel zu weitgehend und würde gegenüber dem rechtlichen Status Quo eher zu einer Verschlechterung führen. So soll die Videoüberwachung sogar zur „Qualitätskontrolle“ zulässig sein, was immer man darunter verstehen mag.

- Es fehlt eine klare Regelung für Fälle, in denen die „gemischte“ dienstliche und private Nutzung von Telekommunikationsdiensten erlaubt ist. Eine solche Regelung könnte auch im Telekommunikationsgesetz verankert werden, allerdings mit dem Nachteil, dass die Regelungen zur Nutzung der dienstlichen E-Mail in diesem Fall in unterschiedlichen Gesetzen geregelt wären.

- Die Regelung, wonach ein Beschäftigter zunächst den Arbeitgeber über Datenschutzverstöße informieren muss, bevor er sich an die Datenschutzaufsichtsbehörde wendet (§ 32l Absatz 4 BDSG-E), beschneidet die Rechte des Beschäftigten unverhältnismäßig.

Der Entwurf befindet sich derzeit in der parlamentarischen Diskussion, in der ich mich weiterhin dafür einsetzen werde, dass der Schutz personenbezogener Daten von Beschäftigten in einer Weise berücksichtigt wird, die den technischen Entwicklungen und den aktuellen Veränderungen in der Arbeitswelt angemessen Rechnung trägt (vgl. zuletzt 22. TB Nr. 11.1).

Die Hoffnung bleibt, dass wir nach Abschluss des Gesetzgebungsverfahrens zum Beschäftigtendatenschutz noch in dieser Legislaturperiode feststellen können: „Was lange gewährt hat, ist endlich gut.“

### 12.2 Datenschutzkontrolle bei der Deutschen Bahn AG – ein Jahrzehnt Arbeitnehmerüberwachung

*Der von der Deutschen Bahn AG in den Jahren 2002 bis 2005 durchgeführte heimliche Datenabgleich bei verdächtigen Mitarbeiterinnen und Mitarbeitern („Datenscreening-Verfahren“) führte zu der Verhängung eines Rekordbußgeldes durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit. Aufgrund meiner gesetzlich eingeschränkten Sanktionsgewalt konnte ich lediglich eine förmliche Beanstandung aussprechen.*

Die Deutsche Bahn AG ist zwar nach der Privatisierung eine nicht-öffentliche Stelle, für deren datenschutzrechtliche Beratung und Kontrolle grundsätzlich der Berliner Beauftragte für Datenschutz und Informationsfreiheit zuständig ist. Soweit die Deutsche Bahn AG allerdings die von der Bundesbahn übernommenen Beamten in ihrem Geschäftsbereich einsetzt, ist sie weiterhin öffentliche Stelle des Bundes und unterliegt meiner datenschutzrechtlichen Zuständigkeit.

Deshalb habe ich zusammen mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit eine gemeinsame datenschutzrechtliche Kontrolle bei der Deutschen Bahn AG durchgeführt. Schwerpunkt war die unrechtmäßige Durchführung und Speicherung der Ergebnisse anlassloser heimlicher Datenabgleichverfahren („Datenscreening-Verfahren“) in den Jahren 2002 bis 2005, bei denen Daten von einer Vielzahl von Beschäftigten und deren Angehörigen mit Daten von Lieferanten abgeglichen wurden. In einzelnen Trefferfällen wurden Mitarbeiterinnen und Mitarbeiter von der Deutschen Bahn AG oder in ihrem Auftrag durch Detekteien vollständig durchleuchtet. Dazu wurden deren Festplatten und die im Netz gespeicherten Dateien kopiert, Büros durchsucht, die Lebensgewohnheiten durch ein privates Ermittlungsbüro überprüft, private Geld- und Kontobewegungen aufgelistet und die Reisetätigkeit und Familienverhältnisse festgehalten. Selbst nachdem sich der Korruptionsverdacht nicht bestätigt hatte, blieben die Ermittlungsberichte und die darin enthaltenen personenbezogenen Daten jahrelang gespeichert. Weiterhin nahm die Deutsche Bahn AG eine systematische Überwachung der E-Mails von Beschäftigten und deren Kontakten vor, um beispielsweise bei kritischen Presseberichten herauszufinden, ob und von wem unternehmensinterne Informationen weitergegeben worden waren. Insbesondere Kontakte zu Journalistinnen und Journalisten, zu Beschäftigten von Bundestagsabgeordneten und zu bekannten Kritikern der Deutschen Bahn AG wurden überwacht.

In dem gegen die Deutsche Bahn AG erlassenen Bußgeldbescheid setzte der Berliner Beauftragte für Datenschutz und Informationsfreiheit ein Bußgeld in der Rekordhöhe von 1,123 Mio. Euro fest. Bei dem diesem Bußgeldbescheid zugrunde liegenden Kontrollbesuch habe ich festgestellt, dass von den Überwachungsmaßnahmen auch beamtete Mitarbeiterinnen und Mitarbeiter der Deutschen Bahn AG betroffen waren. Diese datenschutzrechtlichen Verstöße konnte ich allerdings nur förmlich nach § 25 BDSG i. V. m. § 90 Bundesbeamtengesetz alter Fassung (BBG) beanstanden, weil ich im Gegensatz zu den Datenschutzaufsichtsbehörden der Länder rechtlich keine Möglichkeit habe, Bußgelder zu verhängen (vgl. auch Nr. 2.1).

In einer Folgekontrolle im Jahr 2010 habe ich wiederum Verstöße gegen die §§ 90 ff. BBG a. F. festgestellt. Diese betrafen insbesondere die unzulässige Erhebung, Verarbeitung und Nutzung der Personalaktendaten beamteter Beschäftigter innerhalb des Konzerns. Die Übermittlung der Daten – darunter auch Gesundheitsdaten – erfolgte zum Teil ohne Rechtsgrundlage. Zudem waren die gesetzlichen Löschungsfristen nicht eingehalten worden. Da sich diese Vorfälle auf einen Zeitraum vor meinem ersten Kontrollbesuch im Jahr 2009 bezogen und ich den Umgang der Deutschen Bahn AG mit Personalaktendaten ihrer beamteten Mitarbeiterinnen und Mitarbeiter bereits im damaligen Kontrollbericht beanstandet hatte, habe ich unter Berücksichtigung der Stellungnahme der Deutschen Bahn AG und der ergriffenen Maßnahmen zur Verbesserung des

Datenschutzes darauf verzichtet, die Verstöße erneut zu beanstanden.

Inzwischen hat die Deutsche Bahn AG weitreichende technische und organisatorische und strukturelle Maßnahmen gegen datenschutzrechtliche Verstöße im Unternehmen eingeführt. Der neue Unternehmensvorstand misst dem Datenschutz hohe Priorität zu und hat ein eigenes Vorstandsressort „Compliance, Datenschutz und Recht“ eingerichtet.

So sehr ich diese Maßnahmen begrüße, für so erschreckend und zugleich bedauerlich halte ich es, dass die Führung dieses großen, aus einem staatlichen Sondervermögen hervorgegangenen Unternehmens erst durch die öffentliche Aufmerksamkeit und nach Datenschutzkontrollen, die schwerwiegende Verstöße nachwiesen, die erforderlichen Schritte zur Stärkung des Datenschutzes eingeleitet hat.

## 12.3 Die elektronische Personalakte

*Auch in der Bundesverwaltung dürfen – nach entsprechenden Rechtsänderungen – Personalakten elektronisch geführt werden. Die Verantwortlichen müssen dafür sorgen, dass dabei der Datenschutz gewährleistet bleibt.*

Mit dem am 12. Februar 2009 in Kraft getretenen Gesetz zur Neuordnung und Modernisierung des Bundesdienstrechts (kurz: Dienstrechtsneuordnungsgesetz – vgl. 21. TB Nr. 14.2 sowie 22. TB Nr. 16.15) wurde für die Bundesbehörden erstmalig die Möglichkeit geschaffen, Personalakten der Bundesbeamtinnen und -beamten automatisiert zu führen.

Aus datenschutzrechtlicher Sicht ist die Regelung der elektronischen Personalakte die wesentlichste Neuerung im Bundesbeamtengesetz (BBG). In § 106 Absatz 1 Satz 3 BBG ist nun geregelt, dass die Personalakten der Bundesbeamtinnen und Bundesbeamten sowohl in Schriftform als auch – in Teilen oder vollständig – automatisiert („elektronisch“) geführt werden können.

Die nun grundsätzlich mögliche gemischte Aktenführung teils in elektronischer, teils in Papierform (sogenannte Hybridakten) darf allerdings nicht zu Zweifeln an der Eindeutigkeit der Personalakte und zu Einschränkungen der Rechte der Betroffenen führen. Eine parallele Führung gleicher Aktenteile in Papierform und in elektronischer Form ist daher zu vermeiden. Die personalverwaltende Stelle muss deshalb in den Fällen, in denen die Personalakte nicht vollständig in Schriftform oder vollständig automatisiert geführt wird, nach § 106 Absatz 2 Satz 5 BBG schriftlich festlegen, welche Teile in welcher Form geführt werden. Dies hat sie zudem in dem in die Grundakte aufzunehmenden vollständigen Verzeichnis aller Teil- und Nebenakten zu dokumentieren. Dabei stellen aus zwingenden technischen Gründen vorzuhaltende Sicherheitskopien und Backups aufgrund des materiellen Personalaktenbegriffs keinen Verstoß gegen den Grundsatz dar, dass es nur eine Personalakte geben darf. Aber auch in diesem Zusammenhang ist durch geeignete Maßnahmen jeder Zweifel an der Eindeutigkeit der Personalakte auszuschließen. Für den Betroffenen ist dies zur Sicherstellung seiner Rechte auf Einsicht in seine vollständige Personalakte nach § 110 Absatz 1 BBG von großer Bedeutung.

Sobald die erforderlichen technischen Voraussetzungen vorliegen, insbesondere die Beweiskraft elektronisch gespeicherter Urkunden durch eine qualifizierte elektronische Signatur (§ 3a Absatz 2 Verwaltungsverfahrensgesetz, § 2 Nr. 3 Signaturgesetz) gewährleistet ist, kann die Personalakte auch ausschließlich elektronisch geführt werden.

Im Berichtszeitraum habe ich begonnen, die DRV Bund bei ihren Planungen zur Einführung einer elektronischen Personalakte zu unterstützen (vgl. o. Nr. 5.5).

Da es sich bei den Personalakten stets um besonders schützenswerte Datensammlungen handelt, müssen die zu ihrer elektronischen Führung verwendeten IT-Systeme hohen Sicherheitsanforderungen entsprechen. Ich werde mich deshalb in den kommenden Jahren durch Prüfungen davon überzeugen, ob diese Anforderungen eingehalten werden.

## 12.4 Kontroll- und Beratungsbesuche im Geschäftsbereich des BMVBS

*Im Berichtszeitraum habe ich Beratungs- und Kontrollbesuche im Geschäftsbereich des BMVBS durchgeführt und dabei insbesondere den Umgang mit dem Personalverwaltungssystem PVS BMVBS kontrolliert. In einem Fall musste ich wegen schwerwiegender Mängel bei der IT-Sicherheit eine förmliche Beanstandung aussprechen.*

Beim PVS BMVBS handelt es sich um ein einheitliches Personalverwaltungssystem, das in allen Dienststellen im Geschäftsbereich des BMVBS eingesetzt wird. Dieses konfigurierte und erweiterte SAP R/3 HR-System kombiniert eine zentrale Datenhaltung mit dezentraler Personalverwaltung. Die Betriebsverantwortung für das System liegt beim BMVBS.

Im Rahmen meiner Beratungsaufgabe nach § 26 Absatz 3 BDSG habe ich das BMVBS bei der Entwicklung des PVS BMVBS unterstützt und auf Grundlage des jeweiligen Entwicklungsstandes umfassende datenschutzrechtliche Hinweise und Empfehlungen – auch im Hinblick auf die gesetzlichen Löschungsvorgaben und zu der erforderlichen Dienstvereinbarung – gegeben. Die Besuche im nachgeordneten Bereich dienten dazu, das System erstmalig im Echtbetrieb zu überprüfen. Näheres zum hierbei festgestellten Problem des Löschens von im PVS BMVBS gespeicherten Personal-/Personalaktendaten ist an anderer Stelle dieses TB dargestellt (vgl. Nr. 5.4.2.).

Daneben bin ich bei der Prüfung des Bundesamtes für Seeschifffahrt und Hydrographie (BSH) auf weitere datenschutzrechtliche Probleme und Mängel beim automatisierten Umgang mit Beschäftigtendaten gestoßen. So habe ich im Personalreferat des BSH neben PVS BMVBS 20 bis 30 weitere Verfahren der automatisierten Personaldatenverarbeitung festgestellt, die entgegen den Regelungen in der Dienstvereinbarung und im Einführungserlass des BMVBS ebenfalls für Zwecke der Personalverwaltung/Personalwirtschaft betrieben wurden, für die das BMVBS gerade PVS eingeführt hat. Bereits vor Ort haben meine

Mitarbeiter die Vertreter des Ministeriums gebeten, umgehend alle vorgefundenen Verfahren der automatisierten Personaldatenverarbeitung außerhalb des PVS hinsichtlich ihrer Rechtmäßigkeit zu überprüfen, Notwendiges zu veranlassen und darüber hinaus alle unzulässigen, insbesondere nicht mehr erforderlichen Dokumente und Vorlagen mit personenbezogenen Daten der Beschäftigten zu löschen.

Unter Berücksichtigung der konstruktiven und zügigen Umsetzung meiner datenschutzrechtlichen Hinweise und Empfehlungen, insbesondere der sofortigen Löschung aller unzulässig gespeicherten Personaldaten einschließlich der Personalaktendaten habe ich davon abgesehen, die festgestellten Verstöße gegenüber dem BMVBS formell zu beanstanden.

Auch im Wasser- und Schifffahrtsamt (WSA) Hamburg habe ich die automatisierte Personaldatenverarbeitung unter besonderer Berücksichtigung des Einsatzes des PVS BMVBS überprüft und vergleichbaren datenschutzrechtlichen Handlungsbedarf im automatisierten Umgang mit Beschäftigtendaten festgestellt. Ich begrüße es, dass auch das WSA Hamburg den datenschutzrechtlichen Empfehlungen meiner Mitarbeiter folgend noch während des Besuches reagiert und u. a. alle unzulässig vorgefundenen personenbezogenen Daten der Beschäftigten gelöscht und weitere notwendige Maßnahmen getroffen hat.

Allerdings wurden im WSA Hamburg darüber hinaus erhebliche technisch-organisatorische Mängel festgestellt, etwa der Einsatz von Hack- und Crack-Software auf einem Rechner der Administration sowie eine gespeicherte aktuelle Liste mit Passwörtern der Beschäftigten des WSA Hamburg. Die gefundenen Hack- und Crack-Programme wurden nach Auskunft der Administratoren benutzt, um die vergessenen Passwörter der Kollegen errechnen zu können. Um allerdings bei Erinnerungslücken von Mitarbeitern wieder den Zugang zum System zu eröffnen, muss nur das Passwort durch den Administrator zurückgesetzt werden. Ein Entschlüsseln des Passwortes ist hierzu nicht notwendig. Das Vorhalten und Verwenden von Hack- und Crack-Programmen war unzulässig.

Meine grundsätzliche Haltung zum Einsatz von solchen Programmen möchte ich nochmals darlegen (vgl. auch 20. TB Nr. 4.3.1): Zwar sollten Administratoren über solche Programme informiert sein, der Einsatz dieser Programme in einem IT-System, auf dem auch personenbezogene Daten verarbeitet werden und erst recht in einem bundesweiten Netz stellt allerdings einen groben Verstoß gegen § 9 BDSG dar. Durch den Einsatz von Hack- und Crack-Programmen ist die Sicherheit des gesamten Netzes gefährdet. Ein Einsatz zu Testzwecken kommt deshalb nur in einem separaten Testnetzwerk oder in einem Offline-System in Frage. Soll durch den Einsatz die Sicherheit des Wirkbetriebs getestet werden, müssen die Rahmenbedingungen vorher – auch mit dem Personalrat der Behörde – schriftlich fixiert und abgestimmt werden. Der Einsatz derartiger Programme nur in Abstimmung mit dem IT-Personal und/oder in ständiger Verfügbarkeit ist aus Sicherheitsgründen nicht zulässig.

Weiterhin fand ich ein zur Unterstützung der Mitarbeiter an den Arbeitsplätzen in der Administration eingesetztes Programm, mit dem sich diese „Remote“ auf Arbeitsplätze der Beschäftigten der Behörde aufschalten konnten. Eine Beschreibung des Programms unter Darlegung der Einsatzbedingungen fehlte hier ebenso wie eine Dienstanweisung oder konkrete Regelung der Voraussetzungen zum (zulässigen) Einsatz der Software. Unklar war auch, inwieweit ein Nutzer die Aufschaltung der Administration zur Kenntnis nehmen konnte bzw. aktiv an der Aufschaltung, z. B. durch ausdrückliche Zustimmung (Bestätigung) zur Aufschaltung, mitwirken musste. Unter den vor Ort vorgefundenen Verhältnissen habe ich den Einsatz dieses Tools für unzulässig bewertet.

Aufgrund der umfassenden und schweren technisch-organisatorischen Mängel habe ich die im WSA Hamburg festgestellten Datenschutzverstöße nach § 25 Absatz 1 BDSG gegenüber dem BMVBS beanstandet. Das BMVBS hat das Notwendige veranlasst und mir über die Beseitigung der beanstandeten Mängel berichtet.

### 12.5 Dienstleistungszentren im Bereich der Personalverwaltung

*Bei den im Auftrag des BMI durchgeführten Planungen des Bundesverwaltungsamtes (BVA) zum Auf- und Ausbau von verschiedenen Dienstleistungszentren hat mich das BMI zum vorgesehenen Umgang mit Beschäftigtendaten um datenschutzrechtliche Beratung gebeten.*

Ich freue mich darüber, dass ich im Zuständigkeitsbereich des BMI über ein gutes Beispiel für „Privacy by Design“ berichten kann. Damit wird der Ansatz bezeichnet, etwaige Datenschutzprobleme schon bei der Entwicklung neuer Technologien und Verfahren zu identifizieren und den Datenschutz von vornherein in die Gesamtkonzeption einzubeziehen (vgl. Nr. 3.2). Das BMI hat mich anlässlich seiner Planungen zum Auf- und Ausbau von Dienstleistungszentren (DLZ) für Querschnittsfunktionen/-leistungen sehr frühzeitig um Beratung zum Umgang mit personenbezogenen Daten der Beschäftigten in verschiedenen Projekten bzw. Teilprojekten gebeten. Auf diese Weise können Datenschutzanforderungen schon in einer sehr frühen Phase des Entwicklungsprozesses berücksichtigt werden.

In sehr konstruktiven Beratungsgesprächen, an der auch die Beauftragte für den Datenschutz des BMI teilnahm, konnte ich erste grundsätzliche datenschutzrechtliche Hinweise und Empfehlungen zum vorgesehenen Umgang des BMI bzw. des von ihm beauftragten Bundesverwaltungsamtes (BVA) mit Beschäftigtendaten geben. Die beratende Unterstützung betraf bisher die DLZ-(Teil-)Projekte „Arbeitszeitmanagement“, „Personalgewinnung“, „Personalberichtswesen“, „Rechnungsbearbeitung“ sowie „elektronischer Dienstausweis“. Die Projekte und Planungen zum Auf- und Ausbau der genannten Dienstleistungszentren befinden sich teilweise noch in frühen Entwicklungs- und Planungsstadien. Eine konkrete datenschutzrechtliche Beratung oder gar Bewertung ist zum Teil noch nicht möglich, da wichtige Entscheidungen zum Umgang mit Personaldaten – auch aus personalaktenrechtlicher Sicht – ebenso noch ausstehen wie entsprechende Datenschutz- und Da-

tensicherheitskonzepte. Das BMI hat jedoch zugesagt, meine datenschutzrechtlichen Empfehlungen bei der weiteren Projektarbeit zu berücksichtigen.

Aus datenschutzrechtlicher Sicht ist in diesem Zusammenhang insbesondere von Bedeutung, ob es sich beim Umgang mit Beschäftigtendaten in den geplanten Dienstleistungszentren jeweils um eine Auftragsdatenverarbeitung nach § 11 BDSG oder um eine Funktionsübertragung (Outsourcing) handelt. Davon sind die erforderlichen datenschutzrechtlichen Rahmenbedingungen, deren konkrete Umsetzungen, aber auch meine weitere Beratung im Detail abhängig. Sofern es sich beim Umgang mit Beschäftigtendaten um eine Datenverarbeitung im Auftrag nach § 11 BDSG handelt, sind die entsprechenden Vorgaben des novellierten § 11 BDSG bei der Vertragsgestaltung und im Wirkbetrieb umzusetzen (vgl. Nr. 2.4).

Im Falle des Outsourcing sind neben der Gewährleistung der IT-Sicherheit auch Fragen der rechtlichen Zulässigkeit zu klären, da in dieser Konstellation eine Übermittlung personenbezogener Daten stattfindet, die einer entsprechenden Rechtsgrundlage bedarf.

Ich habe zugesagt, das BMI und das BVA nach Klärung der im Zusammenhang mit dem Umgang mit Personaldaten noch offenen Grundsatzfragen durch das BMI bzw. BVA – je nach entsprechendem Entwicklungsstand – beim Auf- und Ausbau der geplanten Dienstleistungszentren weiterhin zu beraten, um zu einem datenschutzgerechten Umgang mit personenbezogen Daten der Beschäftigten beizutragen.

## 13 Europa und Internationales

### 13.1 Vertrag von Lissabon bringt Änderungen für den Datenschutz

*Das Inkrafttreten des Vertrags von Lissabon stellt einen Meilenstein für die europäische Rechtsentwicklung im Bereich des Datenschutzes dar.*

Der Vertrag von Lissabon, den die 27 Staats- und Regierungschefs der Mitgliedstaaten der Europäischen Union am 13. Dezember 2007 unterzeichneten, trat am 1. Dezember 2009 in Kraft (konsolidierte Fassung im ABl. Nr. C 83 vom 30. März 2010, S. 47 ff.). Mit dem Vertrag wurden die beiden grundlegenden Verträge der Union geändert, der Vertrag über die Europäische Union (EU-Vertrag) und der Vertrag zur Gründung der Europäischen Gemeinschaft (EG-Vertrag), der jetzt Vertrag über die Arbeitsweise der Europäischen Union (AEUV) heißt.

Der Vertrag von Lissabon hat tiefgreifende Änderungen der Systematik des EU-Rechts vorgenommen, indem er die mit dem Vertrag von Maastricht seinerzeit eingeführte Säulenstruktur der Politikbereiche der EU wieder aufhebt. Der bis dahin in Titel VI des EU-Vertrags geregelte Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen („3. Säule“) wurde in den AUEV überführt. Der neue Titel V des AEUV („Der Raum der Freiheit, der Sicherheit und des Rechts“) enthält nun sämtliche Bestimmungen der gemeinschaftlichen Innen- und Justizpolitik (Terrorismusbekämpfung, Politik im Bereich Grenzkontrollen, Asyl und Einwanderung, polizeiliche Zusammenarbeit, justizielle Zusammenarbeit in Zivil- und Strafsachen).

Wichtige Folge der Integration der Justiz- und Innenpolitik in den AEUV ist, dass das ordentliche Gesetzgebungsverfahren nunmehr weitgehend auch für diesen zentralen Bereich der EU-Politik vorgesehen ist und damit die volle Mitentscheidungsbefugnis des Europäischen Parlaments besteht. Für fortbestehende Rechtsakte der Union, die auf Grundlage des Titels VI des alten EU-Vertrags angenommen wurden, besteht indes eine fünfjährige Übergangsfrist ab Inkrafttreten des Vertrags von Lissabon, innerhalb derer das Rechtsschutzsystem der Union weiterhin nur eingeschränkt gilt (Art. 10 Protokoll (Nr. 36) über die Übergangsbestimmungen, ABl. Nr. C 83 vom 30. März 2010, S. 325 f.).

Diese Änderungen, insbesondere der Wegfall der Säulenstruktur, sind auch für den Datenschutz von erheblicher Bedeutung. Mit der Einfügung des Artikel 16 in den AEUV besteht nun eine einheitliche Rechtsgrundlage für den Schutz personenbezogener Daten, die für sämtliche Politikbereiche der EU, einschließlich der polizeilichen und justiziellen Zusammenarbeit, gilt. Artikel 16 Absatz 1 AEUV stimmt wortgleich mit dem Grundrecht auf Datenschutz in Artikel 8 Absatz 1 der EU-Grundrechtecharta (GRCh) überein (vgl. Kasten zu Nr. 13.1). Artikel 16 Absatz 2 AEUV enthält eine Ermächtigungsgrundlage für den Erlass datenschutzrechtlichen Sekundärrechts betreffend die Verarbeitung personenbezogener Daten durch die Organe und sonstigen Stellen der Union sowie die Mitgliedstaaten, soweit diese Tätigkeiten ausüben, die in den Anwendungsbereich des EU-Rechts fallen. Dies hat insbesondere erhebliche Auswirkungen auf den Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit (vgl. Nr. 13.5).

Hinzu kommt, dass mit Inkrafttreten des Vertrags von Lissabon die Charta der Grundrechte der Europäischen Union (GRCh, ABl. Nr. C 83 vom 30. März 2010, S. 389 ff.) durch einen rechtsverbindlichen Verweis in Artikel 6 Absatz 1 des EU-Vertrags in den Rang des Primärrechts gehoben und verbindlich wurde.

Kasten zu Nr. 13.1

**Artikel 8 der EU-Grundrechtecharta: Schutz personenbezogener Daten**

Artikel 8 GRCh enthält das Grundrecht auf Schutz personenbezogener Daten. Absatz 1 garantiert jeder Person das Recht auf Schutz der sie betreffenden Daten. Gemäß Absatz 2 dürfen diese Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Das Grundrecht bindet gem. Artikel 51 Absatz 1 GRCh die Organe und sonstigen Stellen der Union sowie die Mitgliedstaaten bei der Durchführung des Rechts der Union.

## 13.2 Revision der europäischen Datenschutzrichtlinie

*Auch auf europäischer Ebene soll das Datenschutzrecht modernisiert werden. Das wichtigste Vorhaben dabei ist die Überarbeitung des Rechtsrahmens für den Datenschutz in der Europäischen Union.*

Bereits seit 1995 gibt es mit der Richtlinie 95/46/EG eine gemeinsame rechtliche Basis für den Datenschutz in den Mitgliedstaaten der EU. Nach dem Wegfall der Säulenstruktur durch Inkrafttreten des Vertrags von Lissabon (vgl. Nr. 13.1) und durch den rasanten technologischen Wandel ist eine generelle Überarbeitung des europäischen Rechtsrahmens für den Datenschutz dringend erforderlich. Der von der EU-Kommission eingeleitete Reformprozess bietet die Chance, den Datenschutz internetfähig zu gestalten und ihn europaweit auf den Stand des 21. Jahrhunderts zu heben.

Am 9. Juli 2009 hat die Europäische Kommission ein Konsultationsverfahren zum künftigen Rechtsrahmen des EU-Datenschutzes eingeleitet. Die Ergebnisse der Konsultation sollen in den für das 2. Quartal 2011 angekündigten Vorschlag der Europäischen Kommission für eine Neufassung der Datenschutzrichtlinie 95/46/EG einfließen.

Im Rahmen der Konsultation haben die Arbeitsgruppe nach Artikel 29 der Richtlinie 95/46/EG und die Arbeitsgruppe Polizei und Justiz (WPPJ) im Dezember 2009 einen gemeinsamen Beitrag mit dem Titel „Die Zukunft des Datenschutzes“ (WP 168) erstellt. Das Dokument beinhaltet umfassende Vorschläge, um die Grundsätze des Datenschutzes, die Betroffenenrechte und die Stellung der nationalen Datenschutzbehörden zu stärken sowie den EU-Rechtsrahmen auf die Bereiche Justiz und Inneres zu erweitern.

Am 4. November 2010 hat die Europäische Kommission die Mitteilung „Gesamtkonzept für den Datenschutz in der Europäischen Union“, KOM(2010) 609 endg., veröffentlicht. Das Dossier beinhaltet die aus Sicht der Europäischen Kommission wesentlichen Punkte für die Überarbeitung der Datenschutzrichtlinie 95/46/EG. Die Mitteilung befasst sich mit folgenden Schwerpunktbereichen: Stärkung der Rechte des Einzelnen; Stärkung der Binnenmarktdimension; Datenschutz in den Bereichen Polizei und Strafjustiz; globale Dimension des Datenschutzes; Stärkung der Datenschutzbehörden.

(Die genannten Dokumente sind im Internet veröffentlicht unter: http://ec.europa.eu/justice)

Auch im Hinblick auf die Modernisierung des deutschen Datenschutzrechts (vgl. Nr. 1.1) ist die Änderung des EU-Rechtsrahmens von herausragender Bedeutung, bestimmt dieser doch die Spielräume für nationale Regelungen und gibt den Gesetzgebern in den Mitgliedstaaten verbindliche Vorgaben. Deshalb habe ich im Rahmen des Konsultationsverfahrens zur Kommissionsmitteilung über ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“ in Abstimmung mit den Datenschutzbeauftragten der Länder eine Stellungnahme abgegeben. Von zentraler Bedeutung ist dabei die Aussage, dass der Europäische Rechtsrahmen einen hohen Mindeststandard für den Datenschutz vorgeben und zugleich Raum lassen muss für weitergehende Regeln zum Schutz der Betroffenen im Sinne von Artikel 8 der EU-Grundrechtecharta (vgl. Kasten zu Nr. 13.1). Der Konsultationsbeitrag der Datenschutzbeauftragten des Bundes und der Länder ist veröffentlicht auf meiner Internetseite unter www.datenschutz.bund.de in der Rubrik „Europa und Internationales“.

## 13.3 Die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie

*Die Datenschutzgruppe hat wichtige Dokumente im Berichtszeitraum angenommen. Sie erläutern insbesondere für das Datenschutzrecht zentrale Begriffe wie „verantwortliche Stelle“ oder „anwendbares Recht“. Hinzuweisen ist auch auf das Dokument zur Zukunft des Datenschutzes in Europa. Ferner hat die Gruppe eine gemeinsame Kontrolle im Bereich der Vorratsdatenspeicherung durchgeführt und sich zur Angemessenheit des Datenschutz-Niveaus in Andorra, Israel und Uruguay geäußert.*

Die sog. Artikel-29-Gruppe ist das zentrale Koordinierungsgremium für die datenschutzrechtliche Aufsicht in der Europäischen Union. Dieser Gruppe gehören sowohl Vertreter der nationalen Datenschutzaufsichtsbehörden der Mitgliedstaaten als auch der Europäische Datenschutzbeauftragte und – allerdings ohne Stimmrecht – das Datenschutz-Fachreferat der Europäischen Kommission an, das auch die Aufgabe des Sekretariats der Gruppe wahrnimmt.

In den Jahren 2009 und 2010 hat sich die Artikel-29-Gruppe – wie in den Jahren zuvor – mit einer breiten Palette unterschiedlicher Themen befasst. Insgesamt wurden in diesem Zeitraum 22 Dokumente („Working Papers“) von der Gruppe angenommen. Davon wurden 16 Dokumente als offizielle Stellungnahmen („opinion“) der Artikel-29-Gruppe verabschiedet. Die behandelten Themen reichten von datenschutzrechtlichen Fragen bei der Bekämpfung der Produktpiraterie und dem Schutz personenbezogener Daten von Kindern bis zum Datenschutz bei sozialen Online-Netzwerken und der datenschutzrechtlichen Problematik von RFID-Chips.

So hat sich die Artikel-29-Gruppe mit folgenden Stellungnahmen zu bedeutenden datenschutzrechtlichen Fragen geäußert:

- Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten (WP 168) unter dem Titel „Die Zukunft des Datenschutzes“ vom 1. Dezember 2009 (vgl. a. Nr. 13.2).
- Stellungnahme zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ vom 16. Februar 2010 (WP 169). Vor dem Hintergrund der fortschreitenden Entwicklung der Informations- und Kommunikationstechnologien (IKT) und der zunehmenden Globalisierung der Datenverarbeitung ist nach Ansicht der Artikel-29-Gruppe eine Klärung dieser

Begriffe und eine Abgrenzung zum Begriff der „Auftragsdatenverarbeitung“ notwendig. In ihrer Analyse gelangt die Gruppe zu dem Ergebnis, dass die Unterscheidung zwischen verantwortlicher Stelle und Auftragnehmern nach wie vor relevant ist und in der Praxis die Verantwortung stets so zugewiesen werden muss, dass die Einhaltung der Datenschutzbestimmungen hinreichend gewährleistet ist. (zu den Regelungen über die Auftragsdatenverarbeitung im BDSG vgl. Nr. 2.4)

– Stellungnahme zum Grundsatz der Rechenschaftspflicht vom 13. Juli 2010 (WP 173). Zu dem auch unter dem Begriff „Accountability“ bekannten Prinzip der Rechenschaftspflicht bemerkt die Artikel-29-Gruppe, dass die datenschutzrechtliche Verantwortung der verarbeitenden Stelle in der Praxis besser verankert und umgesetzt werden müsse. Diese Notwendigkeit werde nicht zuletzt aus einer Vielzahl von Datenschutzpannen deutlich. Daher entwickelt sie in der Stellungnahme einen konkreten Formulierungsvorschlag für einen Grundsatz der Rechenschaftspflicht, der in die überarbeitete Datenschutzrichtlinie 95/46/EG Eingang finden könnte. Dieser Grundsatz der Rechenschaftspflicht würde die verantwortlichen Stellen dazu verpflichten, angemessene und wirksame Maßnahmen zu ergreifen, um die Grundsätze und Verpflichtungen der Datenschutzrichtlinie für ihren jeweiligen Bereich in der Praxis umzusetzen, und dies auf Verlangen gegenüber den zuständigen Datenschutzaufsichtsbehörden nachzuweisen.

– Stellungnahme zum anwendbaren Recht nach Artikel 4 der europäischen Datenschutzrichtlinie vom 16. Dezember 2010 (WP 179). Die Artikel-29-Gruppe befasst sich in dieser Stellungnahme mit dem Anwendungsbereich der europäischen Datenschutzrichtlinie und insbesondere mit der Frage, unter welchen Umständen das jeweilige nationale Recht eines Mitgliedstaates im Hinblick auf eine Daten verarbeitende, verantwortliche Stelle anwendbar ist. In diesem Zusammenhang werden die Schlüsselbegriffe des Artikel 4 – „Niederlassung im Hoheitsgebiet des Mitgliedstaates“ und „Mittel, die im Hoheitsgebiet des betreffenden Mitgliedstaates belegen sind“ – näher erläutert und mit entsprechenden Beispielen verdeutlicht.

  Eine EU-weite gemeinsame Kontrollaktion der Artikel-29-Gruppe betraf im Berichtszeitraum die Umsetzung der Vorschriften zur Vorratsdatenspeicherung gemäß Richtlinie 2006/24/EG in den einzelnen Mitgliedstaaten. Dabei hat die Artikel-29-Gruppe erhebliche Unterschiede und Mängel festgestellt, insbesondere hinsichtlich der Kategorien der zu speichernden Daten, der notwendigen Sicherheitsmaßnahmen und der Speicherungsfristen. Um diesen Mängeln zu begegnen, werden im Bericht entsprechende Empfehlungen und Handlungsvorschläge abgegeben (WP 172).

Für meine Dienststelle kann ich berichten, dass ein Mitarbeiter des Referates für technologischen Datenschutz die Aufgabe des Koordinators der Arbeitsgruppe „Technology“ der Artikel-29-Gruppe übernommen hat. Daneben sind Angehörige meiner Dienststelle und auch Vertreter der Landesdatenschutzbeauftragten in den übrigen Arbeitsgruppen der Artikel-29-Gruppe engagiert, so dass hier Vorschläge und Erfahrungswissen eingebracht werden können.

Eine chronologisch gegliederte Übersicht der angenommenen Dokumente ist auf der Internet-Seite der Artikel-29-Gruppe einsehbar. Die Dokumente können dort auch in den offiziellen Sprachen der EU elektronisch abgerufen werden. (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm).

## 13.4 Safe Harbor

*Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben auf der Sitzung des Düsseldorfer Kreises am 28./29. April 2010 in Hannover einen wichtigen Beschluss zur Anwendung des Safe-Harbor-Abkommens gefasst.*

Leider sind die Erfahrungen mit dem zwischen der EU und den Vereinigten Staaten von Amerika geschlossenen Safe-Harbor-Abkommen nicht durchgängig positiv. Kritisch sehe ich es insbesondere, dass einige in Europa aktive US-Unternehmen, die sich zur Einhaltung der SH-Prinzipien verpflichtet haben, in ihrer Praxis nicht den Anforderungen des europäischen Datenschutzrechts entsprechen und dass sich die Zusammenarbeit der Datenschutzbehörden mit ihnen teilweise sehr langwierig und kompliziert gestaltet. Dies betrifft insbesondere einige „big Player“ im Internet (vgl. etwa Nr. 4.1.2).

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in ihrem Beschluss vom 28./29. April 2010 darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe-Harbor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss das Daten exportierende Unternehmen klären, ob die Zertifizierung noch gültig ist. Außerdem muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten nach Safe Harbor gegenüber den von der Datenverarbeitung Betroffenen nachkommt. Diese Mindestprüfung müssen die exportierenden Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können.

Die Aufsichtsbehörden betonen ferner die Bedeutung, die einer intensivierten Zusammenarbeit zwischen der auf US-Seite für die Kontrolle des Abkommens zuständigen Federal Trade Commission (FTC) und den europäischen Datenschutzbehörden im Hinblick auf eine verbesserte Einhaltung der Grundsätze zukommt. Die Daten exportierenden Unternehmen werden aus diesem Grund aufgefordert, die zuständige Datenschutzaufsichtsbehörde zu informieren, soweit sie Verstöße gegen Safe-Harbor-Grundsätze feststellen (vgl. Kasten zu Nr. 13.4).

Kasten zu Nr. 13.4

**Sitzung des Düsseldorfer Kreises am 28./29. April 2010 in Hannover**

**Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover**
(überarbeitete Fassung vom 23. April 2010)

**Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen**

Seit dem 26. Juli 2000 besteht eine Vereinbarung zwischen der EU und dem Handelsministerium (Department of Commerce) der USA zu den Grundsätzen des sog. „sicheren Hafens“ (Safe Harbor)[1]. Diese Vereinbarung soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der Safe Harbor-Vereinbarung vorgegebenen Grundsätze verpflichten. Durch die Verpflichtung und eine Meldung an die Federal Trade Commission (FTC) können sich die Unternehmen selbst zertifizieren. So zertifizierte US-Unternehmen schaffen damit grundsätzlich die Voraussetzungen, dass eine Übermittlung personenbezogener Daten aus Europa an sie unter denselben Bedingungen möglich ist, wie Übermittlungen innerhalb des europäischen Wirtschaftsraumes (EU/EWR). Das US-Handelsministerium veröffentlicht eine Safe Harbor-Liste aller zertifizierten Unternehmen im Internet.

Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Harbor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe Harbor-Selbstzertifizierungen vorliegen und deren Grundsätze auch eingehalten werden. Mindestens muss das exportierende Unternehmen klären, ob die Safe Harbor-Zertifizierung des Importeurs noch gültig ist. Außerdem muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten nach Safe Harbor[2] gegenüber den von der Datenverarbeitung Betroffenen nachkommt.

Dies ist auch nicht zuletzt deshalb wichtig, damit das importierende Unternehmen diese Information an die von der Übermittlung Betroffenen weitergeben kann.

Diese Mindestprüfung müssen die exportierenden Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können. Sollten nach der Prüfung Zweifel an der Einhaltung der Safe Harbor-Kriterien durch das US-Unternehmen bestehen, empfehlen die Aufsichtsbehörden, der Verwendung von Standard-Vertragsklauseln oder bindenden Unternehmensrichtlinien zur Gewährleistung eines angemessenen Datenschutzniveaus beim Datenimporteur den Vorzug zu geben.

Stellt ein Daten exportierendes Unternehmen bei seiner Prüfung fest, dass eine Zertifizierung des importierenden Unternehmens nicht mehr gültig ist oder die notwendigen Informationen für die Betroffenen nicht gegeben werden, oder treten andere Verstöße gegen die Safe Harbor-Grundsätze zu Tage, sollte außerdem die zuständige Datenschutzaufsichtsbehörde informiert werden.

Eine Schlüsselrolle im Hinblick auf die Verbesserung der Einhaltung der Grundsätze kommt dabei der Zusammenarbeit der FTC mit den europäischen Datenschutzbehörden zu. Hierfür ist es erforderlich, dass die FTC und die europäischen Datenschutzbehörden die Kontrolle der Einhaltung der Safe Harbor-Grundsätze intensivieren. Die mit der Safe Harbor-Vereinbarung beabsichtigte Rechtssicherheit für den transatlantischen Datenverkehr kann nur erreicht werden, wenn die Grundsätze auch in der Praxis effektiv durchgesetzt werden.

---

[2] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25. August 2000, S. 7.

[3] Informationspflicht: Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

## 13.5 Viel Neues zwischen Stockholm und Lissabon

*In das alte Europa der „3. Säule“ ist viel Bewegung gekommen: ein neues Programm mit neuen Zielvorgaben für die EU und vor allem ein neuer rechtlicher Rahmen nach dem Inkrafttreten des Vertrages von Lissabon.*

Der Rahmen für das, was einmal die „3. Säule“ der Europäischen Union genannt wurde, also der Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, hat sich seit meinem letzten Tätigkeitsbericht grundlegend verändert: So haben sich die Regierungen der Mitgliedstaaten im sogenannten Stockholmer Programm neue politische Zielvorgaben zur weiteren Entwicklung eines Raums der Freiheit, Sicherheit und des Rechts für die nächsten fünf Jahre gesetzt. Dieses Programm weckt aber durchaus zwiespältige Gefühle (vgl. die Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder). Zwar ist der Datenschutz nominell stärker in den Mittelpunkt gerückt, ich habe allerdings angesichts der benannten Vorhaben meine Zweifel, ob sich dies auch in der Arbeit der europäischen Organe niederschlagen wird. Jedenfalls bedarf es weiterer Schritte, um ein ausgewogenes Verhältnis von Sicherheit und Freiheit in Europa zu erreichen (vgl. Kasten zu Nr. 13.5).

Von noch grundlegenderer Bedeutung als das Stockholmer Programm ist allerdings das Inkrafttreten des Vertrages von Lissabon. Die ehemalige Säulenstruktur der EU wurde aufgelöst und die Sonderrolle des Bereichs der polizeilichen und justiziellen Zusammenarbeit in Strafsachen erheblich begrenzt. Zwar bleibt vorerst aufgrund von Übergangsregelungen noch vieles, wie es ist. Doch einiges hat sich schon getan und noch mehr Wandel deutet sich an. Dies liegt nicht zuletzt an Artikel 16 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV), der eine allgemeine Befugnis für den europäischen Gesetzgeber schafft, datenschutzrechtliche Vorschriften auf der Grundlage des neuen Rechtsrahmens im ordentlichen Gesetzgebungsverfahren zu erlassen. Einstimmigkeit ist also nicht mehr erforderlich, das Europäische Parlament ist Organ der Gesetzgebung neben den europäischen Regierungen. Zu diesem Rechtsrahmen gehört nun auch in verbindlicher Form die Grundrechte-Charta, die in Artikel 8 den Schutz personenbezogener Daten als eines der wesentlichen Grundrechte in der EU benennt und zugleich Voraussetzungen für die Datenverarbeitung aufführt (vgl. o. Nr. 13.1).

Hierin sehe ich für den Datenschutz im Bereich der ehemaligen 3. Säule eine besondere Chance. Ziel muss es sein, sowohl das Datenschutzniveau zu verbessern als auch eine stärkere Harmonisierung des Rechts in Europa zu erreichen. Der Rahmenbeschluss über den Schutz personenbezogener Daten bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (vgl. 22. TB Nr. 13.3.1) ist insoweit unzureichend, abgesehen davon, dass er in nur wenigen EU-Mitgliedstaaten bisher umgesetzt wurde. Auf den Prüfstand gehört dabei auch die Art und Weise, wie die nationalen Datenschutzbehörden auf europäischer Ebene zusammenarbeiten. Nach meinem Eindruck will die Europäische Kommission Motor für eine Modernisierung des Datenschutzrechts in der EU sein und den neuen Rechtsrahmen dazu nutzen, die maßgeblichen Rechtsakte für die polizeiliche Zusammenarbeit gründlich zu überholen. Sie hat dies mehrfach angekündigt, zuletzt in ihrer Mitteilung zur Überarbeitung der europäischen Datenschutzrichtlinie 95/46/EG vom November 2010 (vgl. Nr. 13.2). Initiative wie auch das legislative Initiativrecht liegen nun bei ihr.

Gegenwärtig bilden die verschiedenen Rechtsakte im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen ein selbst für Fachleute nur schwer durchschaubares Geflecht. Es wird daher in Zukunft darauf ankommen, allgemeine datenschutzfreundliche Grundsätze für diesen Bereich in der Gesetzgebung zu verankern. Dabei wird es zwar auch weiterhin spezieller Rechtsakte (etwa zum Schengener Informationssystem oder zu Europol) bedürfen. Aber die Abweichungen von den allgemeinen Grundsätzen, etwa beim Auskunftsrecht gegenüber den Polizeibehörden, bedürfen stets der Rechtfertigung und einer normenklaren Ausgestaltung.

Daneben muss die Artikel-29-Gruppe als europäisches Beratungsgremium für Datenschutzfragen infolge der Aufhebung der Säulenstruktur geändert werden. Ihre Begrenzung auf den Anwendungsbereich der Richtlinie 95/46/EG ist schlichtweg nicht mehr zeitgemäß. Darüber hinaus haben die europäischen Datenschutzbehörden einen Weg zu finden, die wichtigen Aufgaben der Kontrolle effektiver zu koordinieren. Deshalb ist auch eine Überarbeitung der Struktur und Arbeitsweise der Kontrollinstanzen notwendig. Die Überlegungen für neue Rechtsregeln im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen stehen noch am Anfang. Ich werde mich bei den anstehenden Diskussionen mit viel Tatkraft einbringen – und in meinem nächsten Tätigkeitsbericht hoffentlich von weiteren Erfolgen berichten können.

Kasten zu Nr. 13.5

**Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. und 9. Oktober 2009 in Berlin**

**Datenschutzdefizite in Europa auch nach Stockholmer Programm**

Die Europäische Union will im Stockholmer Programm ihre politischen Zielvorgaben zur Entwicklung eines Raums der Freiheit, der Sicherheit und des Rechts für die kommenden fünf Jahre festschreiben. Dazu hat die Kommission der Europäischen Gemeinschaften einen Entwurf vorgelegt.

Zwar erwähnt der Kommissionsentwurf die Wahrung der persönlichen Freiheitsrechte und des Schutzes der Privatsphäre als Prioritäten der Innen- und Sicherheitspolitik in einem „Europa der Bürger“. Schritte wie der geplante Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention, Aufklärungs- und Informationskampagnen zum Datenschutz und die Förderung und ggf. Zertifizierung von datenschutzfreundlichen Technologien weisen auch in diese Richtung.

Allerdings bleiben die konkreten Überlegungen für einen verbesserten Datenschutz deutlich hinter den Zielsetzungen für eine verbesserte Sicherheitsarchitektur zurück. Hierzu enthält der Kommissionsentwurf einen umfangreichen Katalog von zum Teil äußerst eingriffsintensiven Maßnahmen, wie z. B. ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der EU oder den Aufbau eines europäischen Strafregisterinformationssystems. Die ebenfalls angestrebte einheitliche Plattform der Informationsverarbeitung mit beinahe beliebigen Datenverarbeitungsmöglichkeiten gefährdet ohne angemessene Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die Bürgerrechte.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder bedarf es weiterer Schritte, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen. Hierzu zählen insbesondere:

– Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.

– Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.

– Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.

– Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.

– Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich für diese Forderungen – auch unter Berücksichtigung der Kritik des Bundesrates etwa zu der Schaffung von Exekutivbefugnissen für EUROPOL und EUROJUST – im weiteren Verfahren einzusetzen.

### 13.6 Ausverkauf von europäischen Finanzdaten an die USA?

*Gegen das sog. EU-US-TFTP-Abkommen zur Übermittlung von Finanzdaten in die USA bestehen Bedenken – auch und soweit das Europäische Polizeiamt Europol in diese Übermittlungen einbezogen ist.*

Meine schwerwiegenden datenschutzrechtlichen Bedenken gegen den Zugriff von US-Behörden auf Überweisungsdaten des Dienstleisters SWIFT habe ich bereits in der Vergangenheit dargestellt (21. TB Nr. 9.4). Das Finanzministerium der USA (US-Treasury – UST) stellt diese Daten in das TFTP (Terrorist Finance Tracking Program) ein, um Aufschluss über die Finanzierung des internationalen Terrorismus zu gewinnen und eigene und fremde Nachrichtendienste und Strafverfolgungsbehörden bei der Prävention und Verfolgung des Terrorismus zu unterstützen.

Die 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in ihrer Entschließung vom 8./9. Oktober 2009 gegen einen „Ausverkauf von europäischen Finanzdaten an die USA“ ausgesprochen und an die Bundesregierung appelliert, die besonders sensiblen Finanzdaten der Bürgerinnen und Bürger wirksam zu schützen und keinem Abkommen zuzustimmen, das eine Datenübermittlung weit unterhalb der Schwelle des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt (vgl. Kasten zu Nr. 13.6).

Am 1. August 2010 ist nun ein modifiziertes EU-US-TFTP-Abkommen in Kraft getreten, das weiterhin erhebliche datenschutzrechtliche Mängel aufweist.

Diese Vereinbarung weist Europol eine Schlüsselrolle zu. Europol soll prüfen, ob die von den USA an SWIFT gerichteten Bitten, dort vorhandene Finanzdaten zu übermitteln, den im Abkommen enthaltenen Vorgaben bzw. Beschränkungen entsprechen. Diese datenschutzrechtliche Kontroll- und Korrektivfunktion wurde Europol aufgrund seiner besonderen Sachkunde zugewiesen. Hierfür darf Europol von US-Behörden – ausschließlich zur Bewertung des Ersuchens – ergänzende Unterlagen anfordern. Nur bei einer entsprechenden positiven Prüfentscheidung wird das an SWIFT gerichtete US-Übermittlungsersuchen wirksam, d. h. nur dann darf SWIFT die angeforderten Daten an die USA übermitteln. Letztlich hängt alles an der

Entscheidung Europols, d. h. an dessen datenschutzrechtlicher Einschätzung.

Besorgniserregend ist, dass Europol einerseits als Wächter fungieren soll, andererseits aber als Polizeibehörde ein Eigeninteresse an der Übermittlung der angeforderten Daten an US-Behörden hat. Denn über die USA können die SWIFT-Daten, die Europol unmittelbar nicht erhalten dürfte, auch dorthin fließen. Zudem verleiht die neue Funktion Europol faktisch die Macht, von US-Behörden auch in anderen Bereichen Daten zu bekommen, die es bis dato nicht (ausreichend) erhalten hat. Diese potentielle Interessenverquickung ist nicht im Interesse der betroffenen Bürgerinnen und Bürger und des Datenschutzes. So ist zumindest fraglich, ob Europol die ihm zugewiesene Kontrollfunktion im Sinne einer Beschränkung des Datenflusses überhaupt erfüllen kann oder will. Dies ist zeitnah zu prüfen. Aus diesem Grund hat das für die Datenverarbeitung Europols zuständige Kontrollorgan, die Gemeinsame Kontrollinstanz (GKI – vgl. o. Nr. 13.11), die Prüfungen der US-Ersuchen durch Europol bereits kontrolliert. Erstaunlicherweise hat Europol wenige Tage vor dieser Kontrolle die US-Ersuchen und alle damit zusammenhängenden Unterlagen als „Geheim“ eingestuft, mit der Folge, dass über konkrete Feststellungen und Ergebnisse dieser Kontrolle öffentlich nicht berichtet werden darf. Details zur weiteren Vorgehensweise der GKI lagen bei Redaktionsschluss noch nicht vor.

Angesichts der herausragenden Kontrollfunktion, die Europol insbesondere vom Europäischen Parlament und der EU-Kommission nach dem Abkommen zugewiesen worden ist, sollten diese Stellen detailliert über die Ergebnisse der GKI-Kontrolle informiert werden. Das gleiche gilt auch für den Rat der EU, den Verwaltungsrat von Europol und die nationalen Parlamente, in denen dieses Abkommen zum Teil sehr kontrovers diskutiert worden ist. Nur dann können ggf. schnell erforderliche Anpassungen vorgenommen bzw. Missbräuche abgestellt werden.

Dies erscheint umso dringlicher, als die EU-Kommission bereits mit Anhörungen zur Einführung eines EU-TFTP begonnen und Europol in diesem Zusammenhang die Möglichkeit gegeben hat, seine Durchführung der Datenschutzkontrolle als ein Modell für das neue EU-TFTP zu präsentieren.

Kasten zu Nr. 13.6

**Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. und 9. Oktober 2009 in Berlin**

**Kein Ausverkauf von europäischen Finanzdaten an die USA!**

Für Zwecke der Terrorismusbekämpfung verhandeln die USA gegenwärtig mit der Europäischen Union über den Zugriff auf Daten über Finanztransaktionen, die auf SWIFT-Servern in Europa gespeichert werden, selbst wenn sie keinerlei Bezug zu den Vereinigten Staaten aufweisen. Besonders kritisch sieht es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass US-Behörden Zugriffsmöglichkeiten auf Transaktionsdaten anstreben, auch wenn gegen die Betroffenen kein hinreichend konkreter Verdacht besteht, dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Ein derartiges Abkommen würde US-Behörden Befugnisse einräumen, die in Deutschland den Sicherheitsbehörden von Verfassungs wegen verwehrt sind.

Ein derartiger weit reichender Eingriff in das Recht auf informationelle Selbstbestimmung weit im Vorfeld des strafrechtlichen Anfangsverdachtes wäre datenschutzrechtlich nicht zu rechtfertigen. Dies wäre auch im Hinblick auf den Vertrauensschutz europäischer Wirtschaftsunternehmen höchst fragwürdig.

Der Datentransfer wäre auch deshalb bedenklich, weil die datenschutzrechtlichen Garantien in den USA deutlich hinter den entsprechenden Anforderungen in der Europäischen Union zurückbleiben. Insbesondere besteht dort keine unabhängige Datenschutzkontrolle; Personen ohne ständigen Wohnsitz in den USA haben kein Recht auf gerichtliche Überprüfung der Verwendung ihrer Daten durch US-Behörden.

Im Übrigen bestehen bereits an der Notwendigkeit eines so weit reichenden Zugriffs ausländischer Behörden auf in Europa gespeicherte Daten erhebliche Zweifel. So können Strafverfolgungsbehörden im Rahmen der Rechtshilfe schon heute einzelfallbezogen personenbezogene Daten zur Aufklärung von Terrorismusverdachtsfällen übermitteln.

Schließlich ist zu befürchten, dass eine derartige Regelung über den Zugriff auf SWIFT-Daten Präzedenzwirkung entfalten würde. Zum einen könnten die Vereinigten Staaten mit derselben Begründung Zugriff auf andere in Europa gespeicherte sensible Datenbestände verlangen, etwa die Vorratsdaten der Telekommunikation. Zum anderen wäre es schwer nachvollziehbar, warum die Europäische Union den USA einen so weitgehenden Zugriff auf in Europa gespeicherte Daten einräumt, entsprechende Forderungen anderer Drittstaaten aber zurückweisen sollte.

Die Konferenz erwartet von der Bundesregierung, dass sie die besonders sensiblen Bankdaten der Bürgerinnen und Bürger wirksam schützt und einem Abkommen nicht zustimmt, das eine Datenübermittlung weit unterhalb der Schwelle des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt.

## 13.7 Datenabgleich mit den Antiterrorlisten

*Auch im Berichtszeitraum beschäftigten mich wieder die Antiterrorlisten der Vereinten Nationen und der EU. Noch immer ist unklar, wer in welchen Fällen und auf welcher Rechtsgrundlage Kunden- und Mitarbeiterdaten mit den Antiterrorlisten abgleichen darf bzw. muss.*

Fragen zum Sinn und zur Rechtmäßigkeit der sogenannten Antiterrorlisten sowie der praktischen Folgen für die gelisteten Personen haben mich schon in meinem letzten Tätigkeitsbericht beschäftigt (vgl. 22. TB Nr. 13.6). Wenngleich sich seitdem einiges getan hat, sind grundlegende Fragen doch weiter offen.

Ungeachtet des fehlenden Nachweises, dass die Antiterrorlisten überhaupt einen signifikanten Beitrag zur Terrorismusbekämpfung leisten, hat sich die Rechtslage für die gelisteten Personen nach der deutlichen Kritik des EuGH durch Überarbeitung der Verordnung ein wenig verbessert. Nach der Verordnung (EU) 1286/2009 vom 22. Dezember 2009 (ABl. L 346 vom 23. Dezember 2009), an deren Beratung ich auf nationaler Ebene vom AA beteiligt wurde, ist der Betroffene nun von seiner Aufnahme in die Liste und den hierfür genannten Gründen von der Europäischen Kommission zu unterrichten und ihm Gelegenheit zur Stellungnahme zu geben. Diese wird dem VN-Sanktionsausschuss zugeleitet. Wie dort mit dieser Stellungnahme weiter verfahren wird, bleibt allerdings ebenso intransparent wie das Listingverfahren innerhalb des Sanktionsausschusses es selbst.

In den Vordergrund der Diskussionen ist zunehmend die Frage gerückt, wer in welchen Fällen und auf welcher Rechtsgrundlage berechtigt und verpflichtet ist, einen Datenabgleich mit den Antiterrorlisten vorzunehmen. Dies ist nach dem Wortlaut der Verordnungen selbst unklar. Es heißt dort lediglich, dass den gelisteten Personen „weder unmittelbar noch mittelbar Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt werden oder zugute kommen“ (Art. 2 Absatz 2 Verordnung (EG) Nr. 881/2002).

Diese und eine vergleichbare Vorschrift richten sich ihrem Wortlaut nach streng genommen an jedermann. Praktisch beschäftigen sich insbesondere die Unternehmen mit der Frage, ob sie einen Abgleich der Mitarbeiterdaten mit den Antiterrorlisten vornehmen bzw. akzeptieren müssen.

Hinzu kommt noch eine Besonderheit für den Bereich des Zollrechts. Wie ich durch zahlreiche Eingaben von betroffenen Unternehmen erfahren habe, haben Zollbehörden die Bewilligung des zollrechtlichen Status eines „Zugelassenen Wirtschaftsbeteiligten“ (Authorised Economic Operator – AEO) von einem systematischen und flächendeckenden Abgleich der Beschäftigtendaten mit den Antiterrorlisten abhängig gemacht. Dagegen habe ich Bedenken. Ich kann in der einschlägigen EG-Durchführungsverordnung Nr. 1875/2006 zum Zollkodex und den diese konkretisierenden Leitlinien der Europäischen Kommission (TAXUD 2006/1450) keine Bestimmung erkennen, die einen systematischen und flächendeckenden Abgleich sämtlicher Beschäftigter mit den EU-Antiterrorverordnungen im Rahmen des zollrechtlichen Zertifizierungsverfahrens legitimiert. Meine Bedenken zu der Praxis der Zollbehörden und der zu Grunde liegenden Dienstanweisung „Zugelassener Wirtschaftsbeteiligter“ (AEO-Dienstanweisung) habe ich dem Bundesministerium der Finanzen (BMF) mitgeteilt.

Das BMF hat daraufhin die einschlägige AEO-Dienstanweisung klarstellend dahingehend geändert, dass ein Abgleich der Beschäftigtendaten anhand der Namenslisten der EU-Antiterrorverordnungen nur für Beschäftigte durchzuführen ist, die „in sicherheitsrelevanten Bereichen“ tätig sind (vgl. AEO-Dienstanweisung, Stand 22. Juni 2010, 253). Einen systematischen und flächendeckenden Abgleich von Beschäftigtendaten darf der Zoll damit von den Unternehmen im Rahmen der AEO-Zertifizierung nicht mehr verlangen. Obwohl mit dieser Einschränkung meinen Bedenken in einem zentralen Punkt Rechnung getragen wurde, empfehle ich weiterhin die Schaffung einer ausdrücklichen gesetzlichen Regelung zum Umfang des zulässigen Datenabgleichs im Rahmen der AEO-Zertifizierung. Denn aus der Praxis höre ich, dass verschiedene Zollämter die genannte Dienstanweisung in sehr unterschiedlicher Art und Weise auslegen.

Der Bedarf für eine gesetzliche Regelung zeigt sich – auch mit Blick auf das Gebot der Verhältnismäßigkeit – daran, dass der Kreis der in sicherheitsrelevanten Bereichen tätigen Beschäftigten unterschiedlich weit gezogen werden kann. Je mehr Beschäftigte dazu zählen, desto weiter wird der Kreis der vom Datenabgleich erfassten Mitarbeiterinnen und Mitarbeiter und umso näher kommt der Datenabgleich einem datenschutzrechtlich bedenklichen, flächendeckenden Mitarbeiterscreening. Um Rechtsklarheit für die betroffenen Unternehmen zu schaffen, empfehle ich eine gesetzliche Regelung, die Art und Umfang der organisatorischen Maßnahmen bestimmt, die ein Unternehmen treffen muss, um seinen Sorgfaltspflichten gerecht zu werden. Wegen der europäischen Dimension der mit der AEO-Zertifizierung verbundenen Fragen, sollte sich die Bundesregierung auch auf europäischer Ebene für eine Konkretisierung der einschlägigen zollrechtlichen EU-Regelungen einsetzen.

Aufgrund der Verunsicherung von Unternehmen und Verbänden bei diesem Thema habe ich die Bundesregierung um Stellungnahme gebeten. Das AA hat mir nach Abstimmung mit den anderen Ressorts daraufhin mitgeteilt, Unternehmen und andere Wirtschaftsbeteiligte seien rechtlich nicht zu einem systematischen, anlassunabhängigen Abgleich ihrer Kunden- und Mitarbeiterdateien verpflichtet. Vielmehr bestehe diese Pflicht ausschließlich nach Maßgabe von Sorgfaltspflichten; eine darüber hinaus gehende Prüfpflicht verstieße gegen den Verhältnismäßigkeitsgrundsatz.

Die Mitteilung des AA sehe ich als einen Schritt in die richtige Richtung an, wenngleich ich befürchte, dass Unternehmen weiterhin unklar sein wird, welche Praxis das Recht gebietet.

Da die Diskussionen um eine etwaige Rechtspflicht zum Datenabgleich und die daraus resultierende Rechtsunsicherheit auf europarechtliche Vorschriften zurückgehen, habe ich zudem die Europäische Kommission um Stellungnahme gebeten, wie die Antiterrorverordnungen aus-

zulegen sind. Eine Antwort auf mein Schreiben steht noch aus.

In der Zwischenzeit ist von verschiedener Seite angeregt worden, einen Runden Tisch einzurichten, um allen betroffenen Akteuren die Möglichkeit einzuräumen, ihren Blick auf das Problem zu äußern, und um gemeinsam eine Lösung zu finden. Ich stehe einem solchen Vorschlag offen gegenüber.

### 13.8 Ein neues Rahmenabkommen mit den USA

*Schon seit Jahren gibt es Kritik am Umgang von US-Behörden mit den Daten europäischer Bürgerinnen und Bürger. Durch ein neues Abkommen mit den USA will die EU nun für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verbindliche Standards auf europäischem Datenschutzniveau setzen.*

Es ist schon beinahe ein Allgemeinplatz, dass die USA ein vollkommen anderes Verständnis von Datenschutz haben. Ob es in der Vergangenheit um die Übermittlung von Fluggastdaten (PNR, vgl. Nr. 13.9), von Finanztransaktionsdaten (vgl. Nr. 13.6) oder von Fingerabdrücken und DNA-Referenzdaten (vgl. 22. TB Nr. 13.4) ging, die Kritik an den USA war allgegenwärtig. Sie richtete sich gegen überlange Speicherfristen, fehlende unabhängige Datenschutzkontrolle oder gegen die fehlende (gerichtliche) Durchsetzbarkeit von Datenschutzrechten europäischer Bürgerinnen und Bürger, um nur einige Punkte zu nennen.

Daher begrüße ich es, dass die europäischen Justiz- und Innenminister Anfang Dezember 2010 der Europäischen Kommission ein Mandat erteilt haben, Verhandlungen über ein Rahmenabkommen mit den USA zu beginnen. In diesem Abkommen sollen die Prinzipien festgelegt werden, die von den jeweiligen Sicherheitsbehörden bei der Übermittlung und Verarbeitung von Daten im transatlantischen Datenverkehr anzuwenden sind.

Aus einem umfangreichen Katalog von Forderungen der europäischen Datenschutzbeauftragten an ein solches Abkommen möchte ich einige, besonders wichtige herausgreifen:

– Um ein durchgehend hohes Datenschutzniveau zu erreichen, müssen die auszuverhandelnden Standards nicht nur für zukünftige Abkommen zwischen der EU und den USA gelten, sondern ebenso für die schon bestehenden. Genauso wichtig ist, dass die neuen Standards auch anzuwenden sind, wenn die einzelnen Mitgliedstaaten auf der Grundlage ihrer nationalen Gesetze bzw. bilateraler Abkommen mit den USA Daten dorthin übermitteln, und zwar unabhängig davon, ob diese bilateralen Abkommen bzw. die nationalen Rechtsgrundlagen schon bestehen oder nicht.

– Es muss sichergestellt werden, dass auch europäische Bürgerinnen und Bürger ihre Datenschutzrechte in den USA gegenüber Behörden und Gerichten durchsetzen können. Insofern sind gegenwärtig erhebliche Zweifel angebracht. Das Abkommen bietet nun die Chance, diese Zweifel durch klare Regelungen zu zerstreuen, die alle amerikanischen Behörden und Gerichte binden und unterschiedslos von der Nationalität der Antragsteller anzuwenden sind.

– Schlicht unvereinbar mit dem europäischen Verständnis von Datenschutz ist die Praxis amerikanischer Sicherheitsbehörden, Daten über viele Jahrzehnte (anlasslos) zu speichern. Dies ist exzessiv und bedarf der angemessenen Begrenzung.

– Eine unabhängige Kontrollbehörde gehört ebenso zum europäischen Grundverständnis von Datenschutz und ist sowohl in der Europaratskonvention 108 als auch in der EG-Datenschutzrichtlinie verankert. Die Rechtsprechung des EuGH hat dies jüngst noch einmal hervorgehoben (vgl. u. Nr. 2.1).

Vieles sieht nach schwierigen und langwierigen Verhandlungen aus. Die Aussicht auf verbindliche Datenschutzstandards beim personenbezogenen Datenaustausch mit den USA lohnt aber diese Anstrengung.

### 13.9 Fluggastdaten

*Die Verwendung von Fluggastdaten für Zwecke der Verhütung und Bekämpfung von Terrorismus und schwerer Kriminalität ist nach wie vor von hoher Aktualität.*

Schon in meinem letzten Tätigkeitsbericht war die Verwendung von Fluggastdaten ein Thema (vgl. 22. TB Nr. 13.5). Die Thematik ist von unveränderter Aktualität: Im September 2010 hat die Europäische Kommission eine Mitteilung zu einer „globalen Strategie“ für den Abschluss von Abkommen über Fluggastdaten vorgelegt. Für einige Bewegung hat auch das Europäische Parlament gesorgt, dessen Zustimmung für Abkommen mit Drittstaaten nach dem Vertrag von Lissabon erforderlich ist. Diese werden nun neu verhandelt (vgl. u. Nr. 13.8.1). Geruht haben indessen bis Redaktionsschluss die Überlegungen im Rat, Fluggastdaten (Passenger Name Records, PNR-Daten) von Passagieren, die aus einem Drittstaat in die EU einfliegen oder in ein solches ausfliegen, auch innerhalb der EU zu verarbeiten und zu nutzen. Die Europäische Kommission hat hierzu für Anfang 2011 einen neuen Vorschlag für einen Rechtsakt angekündigt. Demgegenüber hat die Bundesregierung einen Gesetzesentwurf vorgelegt, der die Fluggesellschaften nach Anforderung zur Übermittlung von Fluggastdaten an die Zollbehörden verpflichten soll. Die Ressortberatungen zu diesem Vorstoß, der nicht der Umsetzung europäischen Rechts dient, waren bei Redaktionsschluss noch nicht abgeschlossen (vgl. u. Nr. 13.8.2).

#### 13.9.1 Neue Entwicklungen zu Abkommen über Fluggastdaten mit Drittstaaten

*Die bestehenden Abkommen über die Übermittlung von Fluggastdaten werden neu verhandelt. Eine entscheidende Rolle wird dabei dem Europäischen Parlament zukommen, dessen Zustimmung nach dem Vertrag von Lissabon erforderlich ist.*

Gegen die undifferenzierte, anlasslose Übermittlung und Verwendung von Fluggastdaten für Zwecke der Gefahren-

abwehr und Strafverfolgung habe ich weiterhin erhebliche Bedenken. Denn hier werden systematisch Daten von in aller Regel unbescholtenen Bürgerinnen und Bürgern aus Buchungssystemen der Fluggesellschaften extrahiert, in andere Staaten übermittelt und dort ohne hinreichenden Schutz und häufig unverhältnismäßig lange gespeichert – und all das ohne einen Nachweis, dass ihre Verarbeitung für Zwecke der Gefahrenabwehr und Strafverfolgung überhaupt sinnvoll und erforderlich ist.

Wiederholt habe ich dabei auf die besonderen Unzulänglichkeiten hingewiesen, die in dem PNR-Abkommen mit den USA enthalten sind (vgl. 22. TB Nr. 13.5). In einem der zentralen Kritikpunkte, dem gewählten Verfahren der Übertragung, bestehen die Defizite fort: Die amerikanischen Behörden bestehen weiterhin auf einem Online-Zugriff auf die Reservierungssysteme der Fluggesellschaften (das sog. Pull-Verfahren), obwohl nach dem Abkommen spätestens bis zum 1. Januar 2008 auf das sog. Push-Verfahren übergegangen werden soll, bei dem die Fluggesellschaften selbst die Daten in die USA übertragen. Hierin sehe ich einen Verstoß gegen die Vereinbarung und erwarte von der EU-Kommission und dem Rat, dass sie gegenüber den US-Behörden auf der vereinbarten Umstellung bestehen.

Im September 2010 hat die Europäische Kommission sowohl eine Mitteilung über die zukünftige „globale Strategie“ zu PNR-Abkommen als auch Richtlinien für Verhandlungen mit den USA, Australien und Kanada über neue PNR-Abkommen vorgelegt. Unter der „globalen Strategie“ versteht die Kommission einen Katalog allgemeiner Voraussetzungen, der für sämtliche PNR-Abkommen mit Drittstaaten gelten soll. Die Art.-29-Gruppe hat in einer Stellungnahme den umfassenderen Ansatz zu PNR-Abkommen und das Eintreten der Europäischen Kommission für einen verbesserten Datenschutz in den Vereinbarungen prinzipiell begrüßt. Allerdings stellt die Gruppe auch die Erforderlichkeit der Verarbeitung von Fluggastdaten durch Sicherheitsbehörden weiterhin in Frage und hat erhebliche Bedenken geäußert, wenn von „Risikoanalysen“ und der „Feststellung von Verhaltensmustern“ aufgrund von PNR-Daten gesprochen wird. Zudem hat sie weitere Verbesserungen zum Schutz des Persönlichkeitsrechts der Passagiere gefordert. Vieles davon entspricht im Übrigen den Forderungen und Bedenken, die auch das Europäische Parlament vorgebracht hat – und auf das Europäische Parlament wird es in Zukunft ankommen. Denn nach dem Vertrag von Lissabon ist dessen Zustimmung für neue Abkommen erforderlich (vgl. Nr. 13.1). Darunter fällt auch das PNR-Abkommen mit den USA, das spätestens 2014 seine Geltung verliert. In der gestärkten Rolle des Europäischen Parlaments liegt eine Chance zur Verbesserung des Datenschutzes im transatlantischen Datenverkehr. Ich hoffe, die Parlamentarier wissen sie zu nutzen.

### 13.9.2 Greift bald auch der Zoll auf Fluggastdaten zu?

*Das Bundesministerium der Finanzen (BMF) will der Zollverwaltung umfangreiche Zugriffsbefugnisse auf Fluggastdaten einräumen. Dem stehe ich kritisch gegenüber.*

In jüngerer Zeit wurden wiederholt Forderungen laut, Fluggastdaten über europarechtlich vorgegebene Verpflichtungen hinaus an zusätzliche Behörden zu übermitteln. So hat das BMF einen Gesetzentwurf vorgelegt, mit dem eine Rechtsgrundlage zur Erhebung und Übermittlung von Fluggastdaten an die Behörden der Zollverwaltung und des Zollfahndungsdienstes geschaffen werden soll. Danach sollen die Zollbehörden weitergehende Zugriffsbefugnisse auf Fluggastdaten erhalten als etwa die Bundespolizei, deren Zugriffsbefugnisse durch europarechtliche Vorgaben (Richtlinie 2004/82/EG – sog. API-Richtlinie, vgl. 22. TB Nr. 13.5.2) bestimmt werden. Beispielsweise soll ein Zugriff auf Fluggastdaten auch bei Flügen aus dem Bundesgebiet in Nicht-EU-Staaten und sogar bei Flügen innerhalb der EU möglich sein. Außerdem ist beabsichtigt, Angaben zur Bezahlung des gebuchten Fluges an die Zollbehörden zu übermitteln. Schließlich sollen umfangreiche Weitergabemöglichkeiten an andere Behörden die Regelung ergänzen.

Diese Entwicklung sehe ich kritisch. Neben meinen grundsätzlichen Bedenken gegen eine anlasslose Weitergabe und Zweckänderung der Fluggastdaten halte ich es für bedenklich, dass nach dem Gesetzentwurf umfassende personenbezogene Daten zu Fluggästen nicht nur an die Zollbehörden, sondern darüber hinaus auch an andere staatliche Stellen übermittelt werden können. Diese Daten könnten zur Profilbildung genutzt oder Raster von Reisenden angelegt werden. Dies ist umso kritischer zu sehen, als nach dem Gesetzentwurf auch Daten von Fluggästen betroffen wären, die zwischen Schengen-Staaten reisen, obwohl gerade Personenkontrollen bei Grenzübertritten im Schengen-Raum weitestgehend abgeschafft wurden.

Die Ressortberatungen, an denen ich erst in einer späten Phase beteiligt wurde, waren bei Redaktionsschluss noch nicht abgeschlossen. Es bleibt zu hoffen, dass die Bundesregierung dieses Vorhaben ad acta legen wird.

### 13.10 Die Umsetzung der „Schwedischen Initiative“

*Die Voraussetzungen für Datenübermittlungen zwischen den europäischen Polizeibehörden sollen den innerstaatlichen entsprechen. Aber das Grundproblem bleibt: Ein gleichwertiges hohes Datenschutzniveau im polizeilichen Bereich fehlt in Europa.*

Nach der „Schwedischen Initiative“ sollen in Zukunft bei der Übermittlung personenbezogener Daten von einer Polizeibehörde eines Mitgliedstaates der EU an eine Polizeibehörde eines anderen Mitgliedstaates keine höheren Anforderungen gelten als bei der Übermittlung an eine andere Polizeibehörde desselben Mitgliedstaates. In einem vereinten Europa klingt das zwar zunächst plausibel, doch setzt dies in allen europäischen Staaten einen möglichst gleichwertigen Datenschutz auf hohem Niveau voraus. Daran fehlt es aber leider nach wie vor.

Die Datenschutzbeauftragten des Bundes und der Länder haben deswegen in ihrer Entschließung vom 6./7. November 2008 (22. TB Nr. 13.3.6) den deutschen Gesetz-

geber aufgefordert, den verbleibenden Spielraum bei der Umsetzung der Schwedischen Initiative datenschutzfreundlich zu nutzen. Mit erheblicher Verzögerung hat die Bundesregierung nun einen Gesetzentwurf in das parlamentarische Verfahren eingebracht, der sich bei Redaktionsschluss noch in einem frühen Stadium der Gesetzgebung befunden hat. Dieser Entwurf, der in seiner Entstehung allerdings viele Entwicklungen genommen hat, setzt das Anliegen in weiten Teilen angemessen um. In den Ressortberatungen habe ich mich unter anderem dafür eingesetzt, dass die Voraussetzungen, wann eine Übermittlung stattfinden kann oder zu versagen ist, klarer geregelt werden und die sog. Spontanauskünfte (also Auskünfte ohne vorheriges Ersuchen) einen engeren Anwendungsbereich haben. Die verbleibenden Defizite sehe ich in erster Linie in der Ungleichzeitigkeit, mit der die Voraussetzungen für einen polizeilichen Datenaustausch verbessert werden, ohne dass zugleich auch die Rechte der Bürgerinnen und Bürger gegenüber Polizeibehörden gestärkt werden. Ich setze insofern viel Hoffnung in den frischen Wind, den der Vertrag von Lissabon gebracht hat (vgl. Nr. 13.5).

## 13.11 Europol

### 13.11.1 Europol – Zentralstelle für den polizeilichen Informationsaustausch in der EU

*Europol entwickelt sich zunehmend zu einer europäischen kriminalpolizeilichen Zentralstelle mit umfassenden Datensammlungen. Dies ist jedoch nur innerhalb des Europol-Beschlusses zulässig.*

Europol hat in den vergangenen Jahren stets an Bedeutung gewonnen. Am 1. Januar 2010 trat mit dem Europol-Beschluss eine neue Rechtsgrundlage in Kraft, mit der auch die Aufgaben und Befugnisse von Europol erweitert wurden (vgl. 22. TB Nr. 13.3.3). Der Vertrag von Lissabon hat die Aufgaben von Europol nun auch im Primärrecht festgeschrieben, und zwar in Artikel 88 des Vertrages über die Arbeitsweise der Europäischen Union. Danach erhält Europol ausdrücklich den Auftrag, die Tätigkeit der Polizei und der Strafverfolgungsbehörden der Mitgliedstaaten und deren Zusammenarbeit bei der Verhütung und Bekämpfung von Straftaten zu stärken. Entsprechend haben sich die Regierungen der Mitgliedstaaten im sog. Stockholmer Programm (vgl. o. Nr. 13.5), das die politischen Ziele für die weitere Entwicklung eines Raumes der Freiheit der Sicherheit und des Rechts benennt, vorgenommen, das Potential von Europol stärker zu nutzen: die Behörde soll verstärkt in den gegenseitigen Informationsaustausch eingebunden werden.

Europol ist deswegen bestrebt, sich als Zentralstelle für den polizeilichen Informationsaustausch in der EU zu positionieren. Auf dem Weg dorthin hat es eine Reihe von Projekten begonnen, mit deren datenschutzrechtlicher Zulässigkeit sich die Gemeinsame Kontrollinstanz von Europol (GKI), die sich aus Vertretern der Datenschutzbehörden der EU-Mitgliedstaaten zusammensetzt, zu beschäftigen hat. Dazu gehören u. a.:

- Das Projekt „Check the web“ (2007 vom EU-Rat der Justiz- und Innenminister beschlossen) zur Vertiefung der Zusammenarbeit der Polizei- und Strafverfolgungsbehörden bei der Beobachtung und Auswertung offener Internetquellen. Kernbestandteil des Projekts war die Einrichtung eines Informationsportals bei Europol als technische Plattform für den sicherheitsbehördlichen Informationsaustausch der Mitgliedstaaten. Im Laufe der Zeit nutzte Europol dieses Portal aber auch dazu, eigene Erkenntnisse darin einzustellen bzw. eigene Analysen mit den darin enthaltenen Informationen zu erstellen. Das Portal wurde damit immer stärker zu einem Europol-Informationssystem. Das Portal wurde daher auf Empfehlung der GKI Europol in den Rechtsrahmen des Europol-Beschlusses überführt und wird fortan als Arbeitsdatei zu Analysezwecken im Sinne des Europol-Beschlusses geführt.

- Unter dem Stichwort „Cross Matching“ prüft Europol die Möglichkeit, inwieweit durch einen Abgleich der bei ihm vorgehaltenen Informationen mit Daten der Mitgliedstaaten, die via Europol ausgetauscht werden, sein Erkenntnisstand erhöht werden kann. In weiteren Schritten ist der Abgleich auch mit Daten aus europäischen Informationssystemen und den nationalen polizeilichen Informationssystemen der Mitgliedstaaten geplant. Derzeitig prüft Europol ausschließlich die von den Mitgliedstaaten unspezifiziert an die Behörde übermittelten Daten im Hinblick auf seine Zuständigkeit sowie zur Klärung der Frage, ob bei Europol bereits Erkenntnisse in den dort geführten Informationssystemen vorhanden sind. Mag die derzeitige Praxis noch im Einklang mit den einschlägigen Regelungen des Europol-Beschlusses stehen, so ist doch zweifelhaft, ob die darüber hinaus gehenden Entwicklungsphasen ohne eine entsprechende Anpassung des Beschlusses rechtskonform verwirklicht werden können.

- Europol hat durch den Europol-Beschluss u. a. auch die Befugnis erhalten, personenbezogene Daten von privaten, kommerziellen Informationsanbietern einzuholen, etwa bei Auskunfteien. Angesichts der Fülle personenbezogener Daten zu in der Regel unbescholtenen Personen, die bei derartigen Auskunfteien vorgehalten werden, darf Europol nur in dem Umfang darauf Zugriff nehmen, wie dies zur Aufgabenerfüllung unbedingt erforderlich ist. Inwieweit insofern die Regelungen des Europol-Beschlusses einen ausreichend präzisen Rechtsrahmen schaffen, bedarf der Prüfung.

Wie diese Beispiele deutlich machen, ist es oft zweifelhaft, ob die angestrebte Entwicklung von Europol hin zu einem Informationsknotenpunkt für die kriminalpolizeiliche Zusammenarbeit in Europa und die dazu eingeleiteten Maßnahmen auf der Grundlage des geltenden Europol-Beschluss verwirklicht werden können. Es handelt sich häufig um neue, eingriffsintensive Formen der Datenverarbeitung, die eher einer spezialgesetzlichen Regelung bedürfen, die Inhalt, Zweck und Ausmaß hinreichend präzisiert und begrenzt.

Vor dem Hintergrund des Bedeutungszuwachses von Europol stellt sich auch die Frage, ob die derzeitige Struktur der Datenschutzkontrolle, die durch eine Gemeinsame Kontrollinstanz aller 27 EU-Mitgliedstaaten wahrgenommen wird, noch zeitgemäß ist und den Anforderungen an eine effektive, effiziente und flexible Datenschutzaufsicht genügt.

### 13.11.2 Beschwerden aus Deutschland im Europol-Beschwerdeausschuss

*Erstmals seit Bestehen des Europol-Beschwerdeausschusses war über zwei Beschwerden aus Deutschland zu entscheiden. Dabei ging es um den Umfang des Auskunftsanspruchs.*

Der Gemeinsamen Kontrollinstanz von Europol (GKI) wurde durch das Europol-Übereinkommen bzw. den Europol-Beschluss u. a. die Aufgabe übertragen, über Beschwerden von Einzelpersonen zu entscheiden, bei denen es um den von Europol erhaltenen Bescheid auf einen Antrag auf Auskunft, Berichtigung oder Löschung geht. Zu diesem Zweck hat die GKI einen Beschwerdeausschuss eingerichtet, der als gerichtsähnliches Gremium ein Rechtsbehelfsverfahren für Einzelpersonen durchführt, die im Zusammenhang mit der Verarbeitung und Nutzung ihrer personenbezogenen Daten durch Europol ihre o. g. Datenschutzrechte einfordern.

Erstmals wurden im Beschwerdeausschuss jetzt auch zwei Beschwerden aus Deutschland verhandelt. Die Beschwerdeführer wandten sich jeweils dagegen, dass Europol es in einer Auskunft ihnen gegenüber offen gelassen habe, ob zu ihnen Daten in den dort geführten Dateien gespeichert seien. Da die Beschwerden noch im Jahr 2009 eingelegt wurden, sind der Entscheidung des Beschwerdeausschusses die insofern einschlägigen Regelungen des Europol-Übereinkommens zugrunde zu legen. Gem. Artikel 19 dieses Übereinkommens muss die Geltendmachung des Auskunftsanspruches sowie die Entscheidung hierüber im Einklang mit den Rechtsvorschriften des Mitgliedsstaates stehen, in dem der Auskunftsanspruch erhoben wurde. Zudem sind die in diesem Artikel bezeichneten Auskunftsverweigerungsgründe zu berücksichtigen. Da in den genannten Fällen die Beschwerdeführer ihr Recht auf Auskunft in Deutschland ausgeübt hatten, gelangte insoweit deutsches Recht zur Anwendung. Danach ergibt sich der Umfang der Auskunftsverpflichtung der verantwortlichen Stelle aus § 19 BDSG. Zur umfassenden Auskunftserteilung gehört es auch, dem Antragsteller mitzuteilen, wenn zu seiner Person keine Daten bei der verantwortlichen Stelle gespeichert sind. Dies folgt unmittelbar aus dem Grundrecht auf informationelle Selbstbestimmung. Informationelle Selbstbestimmung setzt Entscheidungsfreiheit voraus, das Recht auf Löschung oder Berichtigung sowie effektiven Rechtsschutz geltend zu machen. Dies bedingt nicht nur das Wissen darüber, wer welche Daten für welche Zwecke verarbeitet hat, sondern auch ob überhaupt Daten gespeichert sind. Eine Auskunft, die dies offen lässt, trägt der verfassungsrechtlich verankerten Schutzfunktion des nationalen Auskunftsrechts nicht Rechnung. Eine Auskunft und damit auch eine Negativauskunft kann dem Antragsteller nur bei Vorliegen der gesetzlich normierten Auskunftsverweigerungsgründe vorenthalten werden (§ 19 Absatz 4 BDSG). Eine ähnliche Regelung zur Auskunftsverweigerung enthält auch Artikel 19 des Europol-Übereinkommen. Der Beschwerdeausschuss hat demnach zu entscheiden, ob die Auskunftserteilung seitens Europol in den genannten Fällen im Einklang mit den Regelungen des Europol-Übereinkommens und denen des Bundesdatenschutzgesetzes stand. Die Verfahren sind noch nicht abgeschlossen.

## 13.12 Internationale Organisationen

*Sowohl Europarat als auch OECD waren im Berichtszeitraum mit wichtigen Einzelthemen sowie der Vorbereitung einer umfassenden Novellierung ihrer jeweiligen Datenschutzinstrumente befasst.*

Der Europarat nahm im November 2010 eine wichtige Empfehlung zum Thema Profilbildung an, die von den Mitgliedstaaten auf nationaler Ebene umgesetzt werden soll. Die Zusammenführung und Verknüpfung personenbezogener Daten zu Profilen stellt eine besondere Gefährdung der informationellen Selbstbestimmung dar, die zur Wahrung des Persönlichkeitsrechts einer strikten Reglementierung bedarf. Ziel der Empfehlung ist es, einen angemessenen Ausgleich zwischen dem Datenschutz und den legitimen Interessen, die die Erstellung von Profilen rechtfertigen können, zu gewährleisten. Künftiger Arbeitsschwerpunkt des Europarats im Bereich Datenschutz wird die Modernisierung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten („Übereinkommen 108“) von 1981 sein. Mit der geplanten Novellierung des Übereinkommens, die im Frühjahr 2011 mit der Durchführung eines Konsultationsverfahrens beginnen wird, soll insbesondere den aufgrund der technologischen Entwicklungen in Verbindung mit dem Internet hervorgerufenen Herausforderungen, wie etwa Cloud Computing oder sozialen Netzwerken, begegnet werden. Die Modernisierungsbestrebungen stehen insofern in engem inhaltlichen Zusammenhang mit entsprechenden Überlegungen auf Ebene der EU (vgl. Nr. 13.2) und in Deutschland (vgl. Nr. 1.2).

Die OECD feierte bereits 2010 den 30. Jahrestag der Annahme der OECD Privacy Guidelines und richtete aus diesem Anlass drei Jubiläumsveranstaltungen zu den Themen Bedeutung der Guidelines, Rolle des Einzelnen sowie wirtschaftliche Dimension des Datenschutzes aus. Auf der Grundlage des Ergebnisses einer Befragung der Mitgliedstaaten, die für Anfang 2011 geplant ist, soll über eine mögliche Revision der Guidelines entschieden werden. Die OECD hat darüber hinaus auch ihre Bemühungen um eine verbesserte Zusammenarbeit der nationalen Datenschutzbehörden fortgesetzt. Neben der Erarbeitung einer Übersicht nationaler Ansprechpartner und der Erarbeitung eines Standardformulars zur Erleichterung der Kontaktaufnahme zwischen den Datenschutzbehörden unterstützt die OECD die Tätigkeit des „Global Privacy Enforcement Network“ (vgl. o. Nr. 4.11) durch die Entwicklung und Einrichtung der Website des Netzwerks.

### 13.13 Europäische Datenschutzkonferenz

*Die Europäische Datenschutzkonferenz befasste sich im Berichtszeitraum im Schwerpunkt mit Themen aus dem Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen.*

Die Konferenz der europäischen Datenschutzbehörden vom 23. bis 24. April 2009 fand auf Einladung des britischen Datenschutzbeauftragten in Edinburgh statt. Verabschiedet wurde eine Erklärung, die an das Engagement der Datenschutzbehörden für die Wahrung eines hohen Datenschutzniveaus erinnert und hervorhebt, dass Europa auch künftig bei der Förderung des Datenschutzes weltweit eine Führungsrolle wahrnehmen muss (vgl. Anlage 7). In einer weiteren Entschließung werden die europäischen Staaten aufgefordert, beim Abschluss internationaler Abkommen im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen die Einhaltung geltender Datenschutzstandards sicherzustellen (vgl. Anlage 8).

Fragen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen waren auch Gegenstand der Europäischen Datenschutzkonferenz vom 29. – 30. April 2010 in Prag. In einer Entschließung zu dem geplanten Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Datenschutzstandards im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (vgl. o. Nr. 13.8) wird die Europäische Union aufgefordert, sich für ein hohes Datenschutzniveau stark zu machen (vgl. Anlage 9). In einer Entschließung zum Einsatz von Körperscannern für die Sicherheit an Flughäfen betont die Konferenz die Notwendigkeit, einen fairen Ausgleich zwischen der Effektivität und der Notwendigkeit dieser neuen technologischen Geräte und den Auswirkungen auf die Privatsphäre zu gewährleisten (vgl. Anlage 10).

### 13.14 Internationale Datenschutzkonferenz

*Die Internationale Datenschutzkonferenz gab den Anstoß für wichtige Initiativen zur Herausbildung internationaler Datenschutzstandards und der Verbesserung der globalen Zusammenarbeit.*

Die 31. Internationale Datenschutzkonferenz, die vom 4. bis 6. November 2009 in Madrid stattfand, hatte eine Rekordbeteiligung. Mehr als 1 000 Teilnehmerinnen und Teilnehmer aus über 80 Ländern befassten sich mit aktuellen Themen des Schutzes der Privatsphäre. Im Mittelpunkt der Veranstaltung stand die Verbesserung und Vertiefung der internationalen Zusammenarbeit. Besondere Bedeutung soll künftig den gemeinsam mit Industrievertretern und Nichtregierungsorganisationen erarbeiteten internationalen Datenschutzstandards zukommen, die Grundlage eines internationalen Datenschutzübereinkommens werden sollen (vgl. Anlage 11).

Die 32. Internationale Datenschutzkonferenz wurde vom 27. bis 29. Oktober 2010 von der israelischen Datenschutzbehörde in Jerusalem unter dem Motto „Privacy: Generations“ ausgerichtet. Insbesondere am Beispiel der sozialen Netzwerke, wie etwa Facebook oder Twitter, wurden intensiv die unterschiedlichen Anforderungen diskutiert, die verschiedene Generationen an den Datenschutz stellen. Schwerpunktmäßig behandelt wurden auch aktuelle Herausforderungen, die sich dem Datenschutz aufgrund neuer Technologien stellen. In diesem Zusammenhang hat die Konferenz eine Entschließung zum Thema „Privacy by Design“ gefasst, in der sie die frühzeitige Berücksichtigung von Datenschutzanforderungen beim Entwurf informationstechnischer Systeme fordert.

## 14 Aus meiner Dienststelle

### 14.1 Symposium „Moderner Datenschutz im 21. Jahrhundert“

*Am 4. Oktober 2010 fand in Berlin ein viel beachtetes Symposium der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Thema Moderner Datenschutz im 21. Jahrhundert statt. Die organisatorische Vorbereitung der Veranstaltung hatte meine Dienststelle gemeinsam mit den Landesdatenschutzbeauftragten von Baden-Württemberg und Berlin übernommen.*

Die Datenschutzbeauftragten des Bundes und der Länder hatten sich auf ihrer Frühjahrskonferenz im Jahr 2010 darauf verständigt, ein gemeinsames Symposium zu dem verabschiedeten Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ (vgl. o. Nr. 1, Anlage 6) durchzuführen, um die Diskussion über eine grundlegende Modernisierung des Datenschutzrechts in Politik, Gesellschaft und Fachöffentlichkeit voranzubringen.

Die hohe Zahl von nahezu 300 Anmeldungen bewies das überaus große Interesse an der Thematik und trug mit dazu bei, dass sie sehr erfolgreich war und ein positives Resümee gezogen werden konnte.

Das Veranstaltungskonzept sah vor, dass zunächst Redner aus den Bereichen Politik und Technologie mit Fachvorträgen das Thema aus ihrer Sicht betrachten und im Anschluss daran eine Podiumsdiskussion zwischen Politikern, Wissenschaftlern und Vertretern der Wirtschaft unter Beteiligung des Publikums stattfindet. Einzelheiten über den Verlauf des Symposiums, der auch in einem Tagungsband dokumentiert werden soll, sind oben unter Nr. 1 dargestellt. Der Tagungsband war bei Redaktionsschluss noch nicht fertig gestellt. Er wird nach Veröffentlichung über meine Dienststelle zu beziehen und auch auf meiner Internetseite abrufbar sein.

### 14.2 Erfahrungsaustausch mit den behördlichen Datenschutzbeauftragten der obersten Bundesbehörden

*Der regelmäßige Erfahrungsaustausch mit den Datenschutzbeauftragten der obersten Bundesbehörden ist wichtiger Teil der Zusammenarbeit. Das Teilnahmeinteresse ist unvermindert hoch.*

Zur Unterstützung der bei den Dienststellen des Bundes bestellten behördlichen Datenschutzbeauftragten, die sowohl im Interesse der Bürgerinnen und Bürger als auch der Beschäftigten eine wichtige und verantwortungsvolle Aufgabe wahrnehmen, habe ich im Berichtszeitraum den regelmäßigen Erfahrungsaustausch mit den Datenschutz-

beauftragten der obersten Bundesbehörden mit zwei gut besuchten Veranstaltungen im April 2009 und Mai 2010 fortgesetzt. Das regelmäßige Treffen bietet einerseits die Möglichkeit, die von den Teilnehmern für die Tagesordnung angemeldeten Rechtsfragen zu erörtern und über aufgetretene praktische Probleme gemeinsam zu diskutieren, gibt mir andererseits aber auch Gelegenheit, die behördlichen Datenschutzbeauftragten über aktuelle Entwicklungen sowohl im Bereich des Datenschutzes als auch bei der Datensicherheit zu informieren.

Den Erfahrungsaustausch im April 2009 habe ich dazu genutzt, die behördlichen Datenschutzbeauftragten in die Überlegungen über eine grundlegende Modernisierung und Weiterentwicklung des Datenschutzrechts einzubeziehen. Vor dem Hintergrund des von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder geplanten Eckpunktepapiers (vgl. o. Nr. 1) habe ich die Teilnehmer um Mitteilung gebeten, welche Gesetzesänderungen nach ihren Erfahrungen notwendig wären. Erörtert wurden zudem die Themen Auftragsdatenverarbeitung/Outsourcing, private Nutzung von Internet- und E-Mail-Diensten am Arbeitsplatz, Datenschutzaspekte beim elektronischen Terminkalender, Datenschutz beim Einsatz mobiler Datenträger und bestimmter Datenverarbeitungssysteme sowie datenschutzrechtliche Anforderungen an eine Internetpräsenz. Auf der Agenda standen ferner Informationen über das Projekt D 115 (einheitliche Behördenrufnummer) und den Umgang mit Geodaten (Geodatenzugangsgesetz).

Schwerpunktthema der Veranstaltung im Mai 2010 waren die am 1. September 2009 bzw. 1. April 2010 in Kraft getretenen BDSG-Novellierungen, weil sie wichtige neue Vorschriften für das Amt des behördlichen Datenschutzbeauftragten (Stärkung seiner Stellung) und seinen Aufgabenbereich (Anforderungen an Auftragdatenverarbeitung nach § 11 BDSG und deren Kontrolle, Bestimmungen zum Beschäftigtendatenschutz) beinhalteten. Weitere Themen waren u. a. die Kontrolle der Nutzung von Internet- und E-Mail-Diensten sowie der bei der automatisierten Zeiterfassung gespeicherten Daten, die rechtlichen Anforderungen an eine individualisierte Einwilligungserklärung, die Problematik der Auftragsdatenverarbeitung bei Berufsgeheimnisträgern, der Einsatz von Webanalyse-Verfahren, die Sicherheit mobiler Kommunikation in der Bundesverwaltung sowie das Konzept „IT-Steuerung Bund“ und das darin vorgesehene Projekt „Netze des Bundes“.

### 14.3 Aus meiner Dienststelle

*Im Berichtszeitraum habe ich die Öffentlichkeitsarbeit neu ausgerichtet und intensiviert.*

Die Öffentlichkeitsarbeit ist ein wichtiges Mittel, datenschutzrechtliche Themen an den Bürger heran zu tragen und ihn über seine Rechte zu informieren. In Abgrenzung zur Pressearbeit, die eher kurzfristig agiert und reagiert, ist die Öffentlichkeitsarbeit grundsätzlich langfristig und nachhaltig ausgestaltet. Das beinhaltet auch, aktuelle Themen schnell und für jeden verständlich zur Verfügung zu stellen. Insofern verstehe ich die Aufgabe als Dienstleister für den Bürger. Eine enge Zusammenarbeit der drei Bereiche Öffentlichkeitsarbeit, Presse und Internetredaktion ist hierfür Voraussetzung. Zugleich muss die Öffentlichkeitsarbeit von den Fachreferaten als Aufgabe mit hohem Stellenwert innerhalb der Referatsaufgaben angesehen werden.

Mit dem Ziel, die Öffentlichkeit über aktuelle Datenschutzthemen zu informieren, habe ich im Juli 2009 die neue Stabsfunktion „Koordinierung/Lenkung Öffentlichkeitsarbeit“ eingerichtet. In regelmäßigen Abständen legen die aus den einzelnen Fachreferaten benannten Mitarbeiter Art und Umfang, Inhalt sowie Prioritäten öffentlichkeitswirksamer Maßnahmen fest. Neben der notwendigen Bestandsaufnahme bereits veröffentlichter Druckpublikationen (Broschüren und Flyer) wurden neue Ideen entwickelt, von den Fachreferaten inhaltlich umgesetzt und sowohl im Internet als auch in Papierform veröffentlicht. Das Gremium unterstützt mit Rat und Tat die Fachreferate bei der Vorbereitung und Ausrichtung von z. B. Veranstaltungen und Tagungen. Stellvertretend hierfür möchte ich das Symposium „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ erwähnen (vgl. o. Nr. 14.1, 1.4).

Wie in den Jahren zuvor war meine Dienststelle auch wieder beim jährlich in Berlin stattfindenden Tag der offenen Tür mit einem Informationsstand beim Bundesministerium des Innern vertreten. Der persönliche Kontakt und die Möglichkeit, dem Bürger Fragen zu beantworten, aber auch festzustellen, welche Themen die breite Öffentlichkeit interessieren, sind mir wichtig. Ich werde diese Aktivitäten in den kommenden Jahren fortsetzen und weiter ausbauen. Mit der Einrichtung eines Verbindungsbüros in Berlin (vgl. 21. TB Nr. 15.9) war es nun auch möglich, mit anderen Behörden und Institutionen intensiver zusammen zu arbeiten.

Besonders erwähnenswert ist auch, dass meine Mitarbeiter nun auch interessierten Gruppen, die von den Bundestagsabgeordneten zu einer Besuchsreise nach Berlin eingeladen werden, Frage und Antwort stehen. In Zusammenarbeit mit dem Presse- und Informationsamt der Bundesregierung wenden sich immer mehr Abgeordnete aller im Deutschen Bundestag vertretenen Parteien an mein Haus, und bitten, das Thema Datenschutz in ihr Besuchsprogramm aufzunehmen. Trotz der geringen verfügbaren Kapazitäten sind meine Mitarbeiterinnen und Mitarbeiter des Verbindungsbüros gerne bereit, die 90-minütige Veranstaltung durchzuführen. Haben sie im Jahr 2009 insgesamt 18 Besuchergruppen betreut, so konnten im Jahr 2010 fast 30 Vortragswünsche erfüllt werden.

Ob Google Street View oder die Vorratsdatenspeicherung – die Sensibilität für das Thema Datenschutz hat in den vergangenen Berichtsjahren deutlich zugenommen. Dieses verstärkte öffentliche Interesse spiegelt sich auch in der Arbeit meiner Pressestelle wider. Zielsetzung ist es hier weiterhin, die Vertreterinnen und Vertreter der Medien zügig mit adressatengerechten und qualitativ hochwertigen Informationen zu versorgen – sei es durch Hintergrundgespräche, Pressekonferenzen oder Pressemitteilungen. Seit dem 1. Mai 2010 stehen den Journalisten zudem Ansprechpartner in Bonn und Berlin zur Verfügung.

Mit Blick auf den föderalen Aufbau der Datenschutzaufsicht ist es stets erforderlich, übergreifende Themen zwischen den Presseverantwortlichen der Bundes- und Landesdatenschutzbeauftragten abzustimmen. Die Pressestelle hat dies zum Anlass genommen, im September 2010 ein Treffen der Presseverantwortlichen der Bundes- und Landesdatenschutzbeauftragten zu organisieren. Thematisiert wurde unter anderem die Frage, wie die Gefährdung der Persönlichkeitsrechte durch verschiedene Entwicklungen und Vorhaben anschaulicher vermittelt werden kann.

Im Berichtszeitraum wurde mein Internetangebot weiterhin mit steigendem Interesse genutzt, um sich über grundlegende Fragen und aktuelle Entwicklungen im Datenschutzrecht zu informieren (vgl. Kasten zu Nr. 14.3).

Kasten zu Nr. 14.3

**Statistik für das Jahr 2010**

**Internetseite www.datenschutz.bund.de**

| | |
|---|---|
| Seitenaufrufe (gesehener Traffic*) im Jahr 2010 | 9.662.046 |
| Seitenaufrufe (gesehener Traffic*) im Jahr 2009 | 4.604.497 |

* Gesehener Traffic zählt die Aufrufe tatsächlicher Nutzer ohne Berücksichtigung von Robots, Würmern etc.

**Datenschutzforum www.datenschutzforum.bund.de**

| | |
|---|---|
| Zugriffe (im Jahr 2010) | 2.847.080 |
| Beiträge (im Jahr 2010) | 5.553 |
| Beiträge insgesamt (seit Juli 2009) | 9.056 |
| Neue Nutzer (im Jahr 2010) | 908 |
| Nutzer insgesamt (seit Juli 2009) | 2009 |

**Datenschutz-Wiki www.datenschutzwiki.bund.de**

| | |
|---|---|
| Zugriffe (im Jahr 2010) | 125.200 |

**BfDI-Der Film www.datenschutz.bund.de**

| | |
|---|---|
| Zugriffe (im Jahr 2010) | 356.945 |

Darüber hinaus bietet das im Juli 2009 livegeschaltete Datenschutzforum (www.datenschutzforum.bund.de) eine Plattform für den Austausch über den Datenschutz im Betrieb oder im Alltag allgemein. Ergänzt wird dieses Angebot durch meinen Blog, in dem ich anhand von Hintergründen und Erläuterungen eine Orientierung im Umgang mit einer Vielzahl täglicher Datenschutzmeldungen geben möchte.

Einen guten Überblick über meine Aufgaben und Arbeitsweisen können sich interessierte Nutzerinnen und Nutzer auch mit dem neuen Film verschaffen, der auf meiner Internetseite in verschiedenen Formaten angeboten ist. Ob man gegen Datendiebstahl ausreichend gut geschützt ist, verrät der Selbsttest „Datenklau – Sind Sie ausreichend geschützt?“ auf meiner Website. Anhand von elf Sachverhalten aus dem Alltag kann man prüfen, ob man selbst genügend für den Schutz seiner persönlichen Daten tut.

Schließlich habe ich seit kurzer Zeit – einer Forderung aus dem Kreis der Forumsteilnehmer folgend – ein Datenschutz-Wiki (www.datenschutzwiki.bund.de) eingerichtet. Es soll dazu dienen, Begriffe aus allen Bereichen des Datenschutzes (national und international, rechtlich, organisatorisch und technisch, privat und öffentlich etc.) einfach und für jedermann verständlich zu erklären.

## 14.4 Personalaufstockung in der Dienststelle

In den vergangenen Jahren konnte in meiner Dienststelle ein stetiger, starker Anstieg des Aufgaben- und Arbeitsanfalls verzeichnet werden. So haben sich im Jahr 2010 die schriftlichen Eingaben im Verhältnis zum Jahr 2002 fast vervierfacht – von 1647 auf 6087 Eingaben pro Jahr (vgl. Kasten a zu Nr. 14.4). Erreichten meine Dienststelle im Jahr 2008 noch 4 309 schriftliche Eingaben, so stieg die Eingabenzahl in 2009 auf 5 066 und im Jahr 2010 auf 6 087, dies entspricht allein im Berichtszeitraum einem Anstieg um 41 Prozent.

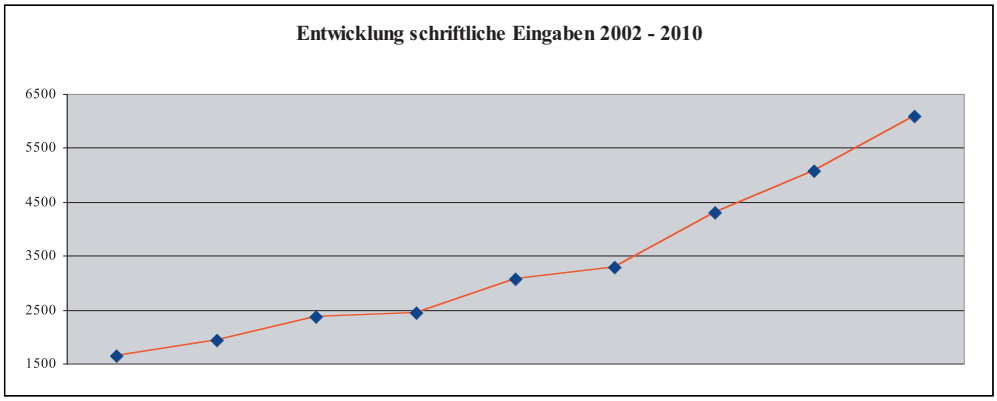
Nachdem in der Vergangenheit die personelle Ausstattung mit dieser Entwicklung nicht Schritt gehalten hatte, erhielt der BfDI im Haushaltsjahr 2010 12,5 neue Personalstellen. Dadurch konnte das Personalsoll von 69 Stellen im Jahr 2008 auf 81 Stellen in 2010 erhöht werden (vgl. Kasten b zu Nr. 14.4).

Das zusätzliche Personal ermöglicht es meiner Dienststelle, die bestehenden gesetzlichen Aufgaben besser zu bewältigen und neue Aufgaben aktiv aufzugreifen. Der Stellenzuwachs machte es zudem möglich, die Organisation meiner Dienststelle an aktuelle Entwicklungen anzupassen. So konnte insbesondere die Kompetenz im technologischen Datenschutz deutlich ausgebaut werden, um mit den gestiegenen Anforderungen in diesem Bereich Schritt halten zu können. Daneben soll meine Kontroll- und Aufsichtsaufgabe intensiviert werden.

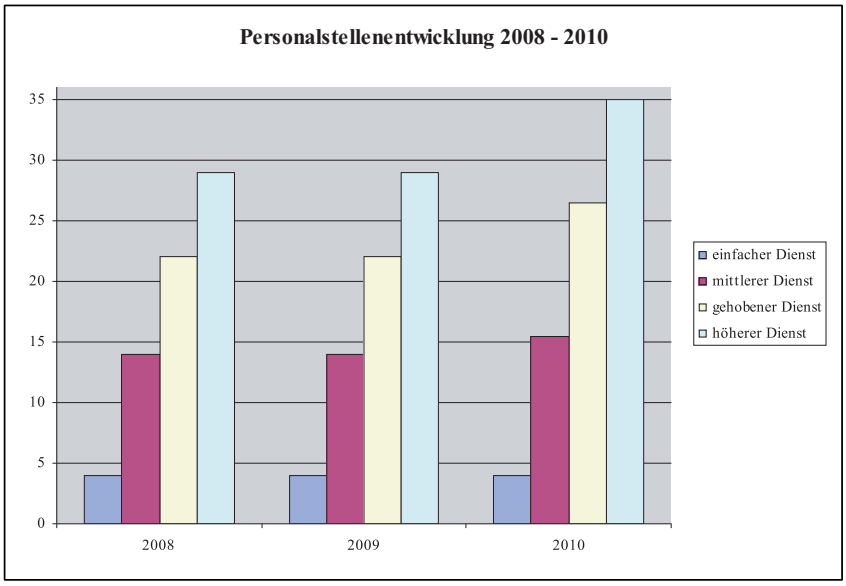
Kasten a zu Nr. 14.4

**Eingaben /Petitionen**

| Jahr | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|---|
| Anzahl | 1647 | 1927 | 2376 | 2449 | 3067 | 3295 | 4309 | 5066 | 6087 |




Kasten b zu Nr. 14.4



## 14.5 Meine Präsenz in Berlin

*Das Verbindungsbüro in Berlin vergrößerte sich in den Jahren 2009 und 2010.*

Um die Präsenz meiner Dienststelle in Berlin zu erhöhen, wurde Anfang 2008 in der Friedrichstraße 50 in Berlin-Mitte ein Verbindungsbüro eingerichtet. Seine vorrangigen Aufgaben bestehen in der Koordinierung und Wahrnehmung von Terminen, insbesondere in den Ausschüssen des Deutschen Bundestages sowie in den Sitzungen der Bundesressorts in Berlin. In den Jahren 2009 und 2010 konnte das Verbindungsbüro vergrößert werden. Neben mir ist es nunmehr mit dreizehn Mitarbeiterinnen bzw. Mitarbeitern besetzt. Es erfüllt somit größtenteils das mit der Konzeption verfolgte Ziel, wonach jedes Referat im Verbindungsbüro vertreten sein soll. Nach jetzigem Planungsstand wird die Konzeption im Laufe des Jahres 2011 umgesetzt sein.

Das Verbindungsbüro hat sich hervorragend bewährt. Seit Inbetriebnahme konnten zum großen Teil die Termine in Berlin von Mitarbeiterinnen und Mitarbeitern des Verbindungsbüros wahrgenommen werden, wodurch eine wirkungsvollere und direktere Teilnahme am politischen Geschehen in der Bundeshauptstadt erreicht wird. Den Referaten konnten dadurch zeitaufwändige Dienstreisen zur Terminwahrnehmung erspart werden.

## 14.6 Forschungsprojekte sollen Datenschutz voranbringen

*Haushaltsmittel für gezielte Forschung auf den Gebieten des Datenschutzes und der Informationsfreiheit.*

Erstmals im Haushaltsjahr 2010 wurden mir Haushaltsmittel für Forschungs- und Entwicklungsvorhaben auf dem Gebiet des Datenschutzes und der Informationsfreiheit in Höhe von 100 000 Euro bewilligt. In diesem Rahmen habe ich folgende Forschungsvorhaben angestoßen:

– Erstellung eines Leitfadens zur Evaluation von Gesetzen

  In den letzten Jahren wurde in zunehmendem Maße Kritik an der Wirksamkeit von Gesetzen geübt. Auch die Politik hat dieses Thema aufgenommen; die Evaluierung von Gesetzen hat inzwischen eine hohe Priorität. Obwohl die Evaluierung in der Entwicklungszusammenarbeit oder in der Sozial- und auch Wissenschaftspolitik eine bewährte Praxis darstellt, existieren bislang wenig konkrete Vorschriften. So soll mit diesem Forschungsprojekt ein Leitfaden für Evaluierung erstellt werden, mit besonderem Blick auf Gesetze, die mit Eingriffen in den Datenschutz verbunden sind.

– PRIVIDOR – PRIvacy Violation DetectOR

  Dem Benutzer des Internet bleibt oftmals verborgen, welche Einstellungen bzw. Informationen im Hintergrund von Web-Anwendungen gespeichert werden. Daher soll mit diesem Forschungsprojekt ein Tool mit entsprechender Benutzeroberfläche entwickelt werden, um automatisch Websites daraufhin zu testen, ob diese Cookies/Flash-Cookies etc. setzen oder andere datenschutzproblematische Vorgänge durchgeführt werden. Das Tool soll die wichtigsten datenschutzrechtlichen Problembereiche, welche explizit unter „Berücksichtigte datenschutzrelevante Vorgänge“ aufgeführt werden, überprüfen und einen Report erzeugen. Ziel ist es, das Tool nach der Entwicklung interessierten Stellen und allen Bürgerinnen und Bürgern zur Verfügung zu stellen.

– Informationsfreiheit und der Schutz der Betriebs- und Geschäftsgeheimnisse

  Seit Inkrafttreten des Informationsfreiheitsgesetzes wurde immer wieder Bürgerinnen und Bürgern der Informationszugang mit der Begründung verweigert, es handle sich um Betriebs- und Geschäftsgeheimnisse. Eine entsprechende Legaldefinition sieht das Gesetz nicht vor, auch keine Negativabgrenzung, was kein Betriebs- und Geschäftsgeheimnis ist. Ziel des Forschungsprojekts ist es, Zweck und Reichweite des Schutzes von Betriebs- und Geschäftsgeheimnissen in den verschiedenen Rechtsgebieten herauszuarbeiten und einen praktischen Ansatz für einen Lösungsvorschlag zu erstellen.

Zwischenergebnisse konnten schon Ende 2010 erreicht werden, mit einem Abschluss der Forschungsprojekte rechne ich im Laufe des Jahres 2011.

## 14.7 BfDI als Ausbildungsbehörde

*Referendare, Praktikanten und Anwärter.*

Wie bereits in den vergangenen Jahren war erneut großes Interesse an Praktikumsaufenthalten in meiner Dienststelle festzustellen, insbesondere von Studierenden der Rechtswissenschaften und Rechtsreferendaren, die sich für Fragen des Datenschutzes und der Informationsfreiheit interessierten und praktische Kenntnisse erwerben wollten.

Insgesamt haben im Jahre 2009 und 2010 fünfundzwanzig Studierende und Referendare Teile ihrer Ausbildung in meinem Hause absolviert. Darüber hinaus konnte ich drei Anwärterinnen und Anwärtern des gehobenen Dienstes in der allgemeinen inneren Verwaltung die Möglichkeit bieten, ihr Pflichtpraktikum in meiner Dienststelle abzuleisten.

Angesichts der uneingeschränkt positiven Erfahrungen werde ich auch künftig alle Möglichkeiten nutzen, an der Ausbildung mitzuwirken.

## 14.8 Fortentwicklung der elektronischen Akte

Bereits vor mehr als zehn Jahren hat mein Amtsvorgänger in seinem 18. TB (Nr. 33.4.1) sowie im 19. TB (Nr. 33.9) von der Einführung elektronischer Akten unter Nutzung eines DOMEA-zertifizierten Dokumentenmanagementsystems in der Dienststelle berichtet.

Nach dem Aufbau des elektronischen Archivs ab dem Jahre 2001 folgten Jahre paralleler Aktenführung – neben der vollständig geführten, verbindlichen Papierakte existierte eine 1:1-Abbildung als elektronische Ablage.

Im Jahr 2010 konnte nun ein wichtiger Schritt auf dem Weg zur ausschließlich elektronisch geführten Akte vollzogen werden. Die an mich gerichteten Eingaben von Bürgerinnen und Bürgern machen einen wesentlichen, jährlich stetig anwachsenden Anteil der Geschäftsvorfälle aus (vgl. Kasten zu Nr. 14.4). Um die Arbeit effektiver zu gestalten, werden diese nicht mehr herkömmlich in Papiervorgängen, sondern ausschließlich in elektronischer Form bearbeitet. Die Eingaben sind hier besonders geeignet, weil je Geschäftsvorfall nur eine relativ geringe Anzahl an Dokumenten erzeugt wird und diese regelmäßig innerhalb eines kurzen Zeitraums abgearbeitet werden können. Vielfach können einfache Fälle durch mein Servicebüro erledigt werden, wenn es sich um häufig wiederkehrende, routinemäßige Anfragen handelt. Hierdurch wird das betreffende Fachreferat erheblich entlastet und kann sich stärker auf die fachlichen Kernaufgaben konzentrieren.

Die bestehende Aufteilung meiner Dienststelle mit Hauptsitz in Bonn und einem Verbindungsbüro in Berlin verlangt geradezu nach einer Möglichkeit, Arbeitsergebnisse standortübergreifend und ohne Zeitverzug mittels moderner Informations- und Kommunikationstechnik zu erbringen. Die vollelektronische Bearbeitung der Eingaben hat erwiesen, dass die Arbeit nicht nur schneller, sondern auch in höherer Qualität erledigt wird. Die anfangs bei den Beschäftigten teilweise noch bestehenden Vorbehalte konnten durch die erzielten positiven Ergebnisse grundsätzlich ausgeräumt werden. Basierend auf den guten Erfahrungen werden ab 2011 sukzessive weitere Geschäftsprozesse in die vollelektronische Bearbeitung überführt.

Über den Fortgang des Projekts werde ich auch künftig berichten.

## 15 Wichtiges aus zurückliegenden Tätigkeitsberichten

1. 22. TB Nr. 5.7 **Einrichtung einer Visa-Warndatei**

   Der Ankündigung im Koalitionsvertrag für die 17. Legislaturperiode folgend hat das Bundesministerium des Innern einen Referentenentwurf zur Schaffung einer zentralen Visa-Warndatei vorgelegt. Zwar wurde darin die noch in der vergangenen Legislaturperiode vorgesehene generelle und verdachtsunabhängige Speicherung von Daten zu Einladern, Verpflichtungsgebern und Bestätigenden nicht wieder aufgegriffen. Gleichwohl gehen einzelne der beabsichtigten Warnsachverhalte, die eine Speicherung in der Datei auslösen, über das erforderliche Maß hinaus. Dies betrifft etwa die beabsichtigte Speicherung bei einem bloßen Verdacht rechtswidrigen Verhaltens. Kritisch bewerte ich auch, dass Straftaten gespeichert werden sollen, die weder in einem Zusammenhang zum Visumverfahren stehen noch einen sonstigen Auslandsbezug aufweisen. Zudem sind nach dem Referentenentwurf weitreichende Zugriffsbefugnisse für die Sicherheitsbehörden vorgesehen. Im Rahmen meiner Beteiligung in der Ressortabstimmung habe ich meine Bedenken gegen die beabsichtigte Ausgestaltung der Visa-Warndatei deutlich gemacht. Soweit das Vorhaben einer zentralen Visa-Warndatei weiterverfolgt wird, sollte diese in erster Linie die deutschen Visumsbehörden bei ihrer Tätigkeit unterstützen. Welche Daten in einer solchen Datei gespeichert werden, sollte sich ausschließlich an diesem Zweck orientieren. Es bleibt abzuwarten, wie das Vorhaben weiter umgesetzt wird.

2. 22. TB Nr. 7.5 **Jobbörse als Internet-Angebot der Bundesagentur für Arbeit**

   Obwohl ich die Bundesagentur für Arbeit (BA) ausdrücklich auf die Missbrauchsanfälligkeit des Registrierungsverfahrens für Arbeitgeber bei ihrer Online-Jobbörse hingewiesen hatte, reagierte die BA hierauf zunächst nicht. In der Folgezeit gelangte tatsächlich eine Vielzahl unseriöser Stellenangebote in die Jobbörse. Zum Beispiel stellte eine Firma für Personalvermittlung mehrere Tausend vermeintliche Stellenangebote aus unterschiedlichen Berufssparten allein mit dem Ziel in die Jobbörse ein, dadurch an Bewerberdaten für eigene Vermittlungsgeschäfte zu gelangen.

   Erst diese spektakulären Datenmissbrauchsfälle und die damit verbundenen öffentlichen Diskussionen veranlassten die BA, die fälligen Schutzvorkehrungen zu treffen. Jeder neue Arbeitgeber wird nun vor einer Registrierung überprüft. Dies erfolgt zusätzlich zu einer stichprobenartigen Plausibilitätskontrolle von eingestellten Stellenangeboten. Geprüft werden die Arbeitgebereigenschaft, die Branchenzugehörigkeit und die Korrektheit der gemachten Angaben. Auch den Bestand von etwa 40 000 bereits registrierten Arbeitgebern hat die BA auf meine Forderung hin sukzessive nachträglich überprüft. Dabei mussten nach Angaben der BA etwa 6 Prozent zweifelhafte Arbeitgeber-Accounts gelöscht werden.

   Auch wenn sich Missbrauch in derartigen Online-Portalen nie völlig ausschließen lässt, so ist gleichwohl das höchstmögliche Datenschutzniveau zu gewährleisten. Dies gilt umso mehr, als hier Sozialdaten betroffen sind. Durch eine rechtzeitige Berücksichtigung meiner Anregungen hätten sich viele Missbrauchfälle vermeiden lassen.

3. 22. TB Nr. 10.5.1 **Erhebung von Merkmalen des Migrationshintergrundes von Arbeitsuchenden**

   Ich hatte über die neu geschaffene Regelung des § 281 Absatz 2 SGB III zur Erhebung von Merkmalen des Migrationshintergrundes von Arbeitsuchenden ausschließlich zu statistischen Zwecken berichtet. Die entsprechende Rechtsverordnung ist seit Oktober 2010 in Kraft (BGBl. 2010 I S. 1372). Sie sieht auch eine Regelung zur Binnendifferenzierung von Spätaussiedlern vor. Die Gesetzesbegründung, über diese Gruppe auch im Bereich der Arbeitsmarkt- und Grundsicherungsstatistiken genaue Zahlen zu erhalten, um die Integration voranzutreiben, halte ich für schlüssig.

   Die Pläne zur Verwendung der Daten über den Migrationshintergrund auch im operativen Geschäft sind in der zurückliegenden Legislaturperiode gescheitert und bislang nicht wieder aufgegriffen worden.

4. 22. TB Nr. 14.2 **Datenschutz in deutschen Auslandsvertretungen**

   Die bei einem Kontroll- und Beratungsbesuch festgestellten datenschutzrechtlichen Defizite in einer deutschen Auslandsvertretung wurden inzwischen durch das Auswärtige Amt (AA) zum größten Teil beseitigt. Zu dem noch offenen Punkt des bislang nicht geführten Verzeichnisses der Datenverarbeitungsanlagen hat mir das AA nunmehr mitgeteilt, dass es derzeit an einer Integration eines Verzeichnisses der Datenverarbeitungsanlagen in ein neues Formularsystem arbeite. Erörterungsbedürftig ist weiterhin auch die Absicherung der Kommunikation der Rechts- und Konsularbereiche der Auslandsvertretungen mit den deutschen Behörden über das Internet. Da damit im Wesentlichen die Kommunikation mit Landes- bzw. Kommunalbehörden (z. B. Meldeämtern) betroffen ist, habe ich die Landesbeauftragten für den Datenschutz an der Diskussion beteiligt. Die Abstimmung mit ihnen war bei Redaktionsschluss noch nicht abgeschlossen.

5. 21. TB Nr. 13.1.3 **Selbstauskunftsbögen** und **Krankenhausentlassungsberichte**

   In den vergangenen Tätigkeitsberichten habe ich mich wiederholt mit der Frage auseinandersetzen müssen, wie weit die Erhebungsbefugnisse gesetzlicher Krankenkassen im Hinblick auf medizinische Daten bei Selbstauskunftsbögen (21. TB Nr. 13.1.3) und Krankenhausentlassungsberichten (18. TB Nr. 21.3) reichen. Die Problematik beschäftigt mich weiterhin. Einige Krankenkassen haben zugesichert, sich bei der Vordruckgestaltung nur noch an Vordruckvereinbarungen (z. B. zur sozialmedizinischen Beratung und bei Arbeitsunfähigkeit) mit dem Medizinischen Dienst des Spitzenverbandes Bund (MDS) zu orientieren. Zahlreiche Krankenkassen lassen sich jedoch nach wie vor zu unterschiedlichen Anlässen, wie z. B. bei Krankengeldbezug, Versorgung mit Hilfsmitteln, anstehenden Reha-Maßnahmen, Selbstauskunftsbögen ausfüllen. Die mir vorliegenden Fragebögen enthalten regelmäßig umfassende Schweigepflichtentbindungserklärungen, die behandelnde Hausärzte befugen, ärztliche Aufzeichnungen, erhaltene Krankenhausentlassungsberichte, fachärztliche Gutachten etc., der Krankenkasse zu überlassen.

   In Gesprächen mit den Beteiligten (BMG, Bundesversicherungsamt, Spitzenverbände der Krankenkassen) wurden die verschiedenen Positionen noch einmal diskutiert und mögliche Lösungswege ausgelotet. Diese Gespräche werden fortgesetzt und ich hoffe, dass dabei eine alle berechtigte Interessen ausgleichende Lösung gefunden wird.

6. 22. TB Nr. 6.1.2 **Statuskennzeichen auf der Krankenversichertenkarte**

   Ich habe darüber berichtet, dass die Krankenversichertenkarte durch den Aufdruck einer bestimmten Ziffer (Ziffernstelle 4) in codierter Form die Statusergänzung „Sozialhilfeempfänger“ ausweist, ohne dass es hierfür eine Rechtsgrundlage gibt. Zwar müssen die Krankenkassen zu Abrechnungszwecken Kenntnis über den Status ihrer Mitglieder erhalten. Dies ist aber nicht zwingend über die Versichertenkarte zu gewährleisten. Bis zur Einführung der elektronischen Gesundheitskarte (vgl. hierzu Nr. 3.4), mit welcher dieses Problem gelöst wird, hat das Bundesministerium für Gesundheit als Übergangslösung vorgeschlagen, die Ziffernstelle auf der Versichertenkarte, die die Statusergänzungen ausweist, zu generalisieren. Der GKV-Spitzenverband hat versichert, den Vorschlag auf seine Umsetzbarkeit zu prüfen. Bisher liegt jedoch noch keine abschließende Antwort vor.

7. 22. TB Nr. 10.2.4 **Verstöße von Krankenkassen bei der Vermittlung privater Zusatzversicherungen**

   Aufgrund der außergewöhnlich schweren datenschutzrechtlichen Verstöße zweier gesetzlicher Krankenkassen bei der Kooperation mit einer privaten Krankenversicherung zum Zweck der Vermittlung privater Zusatzversicherungen an ihre Versicherten hatte ich sowohl gegen Mitarbeiter beider gesetzlicher Krankenkassen als auch gegen Mitarbeiter des privaten Versicherungsunternehmens bei den zuständigen Staatsanwaltschaften Strafantrag nach § 85a Absatz 2 SGB X wegen Vergehen nach § 85a Absatz 1 i. V. m. § 85 Absatz 2 Nummern 1, 2, 3 und 5 SGB X gestellt. Die gesetzlichen Krankenkassen hatten mit ihnen verbundenen privaten Krankenkassen Zugang zu zum Teil sehr sensiblen Daten ihrer Versicherten verschafft. In beiden Fällen dauern die staatsanwaltlichen Ermittlungen auch drei Jahre nach Stellung der Strafanträge noch an.

8. 22. TB Nr. 3.4.1 **Europäische Dienstleistungsrichtlinie (Einsatz des Europäischen Binnenmarktinformationssystems IMI):**

   Die EG-Dienstleistungsrichtlinie ist zum 28. Dezember 2009 umgesetzt worden. In den Bundesländern stehen die sog. Einheitlichen Ansprechpartner potentiellen Dienstleistungserbringern mit Rat zur Verfügung.

   Zur europaweiten Amtshilfe ist auch das Binnenmarktinformationssystem IMI Anfang 2010 ans Netz gegangen. Eine Vielzahl von Behörden kann nun miteinander elektronisch kommunizieren, wenn z. B. Zweifel an der Echtheit der vom Dienstleistungserbringer vorgelegten Unterlagen bestehen und deshalb bei den zuständigen Behörden in dem ausstellenden Mitgliedstaat Nachfragen erforderlich werden.

   Der Forderung der Datenschutzbeauftragten des Bundes und der Länder sowie des Europäischen Datenschutzbeauftragten, den Betrieb von IMI auf eine klare Rechtsgrundlage zu stützen, ist die Europäische Kommission zwar noch nicht nachgekommen, hat eine solche jedoch inzwischen in Aussicht gestellt.

   Die Anzahl der über IMI abgewickelten Anfragen ist (erwartungsgemäß) nicht sehr hoch, so dass mittlerweile Überlegungen angestellt werden, die vorhandene technische Infrastruktur auch auf ausschließlich nationaler Ebene zu nutzen. Für die interne Verwendung von IMI fehlt nicht nur eine Rechtsgrundlage;

auch aus anderen Gründen würde dies zu enormen Problemen führen. Da der zentrale Server von der Europäischen Kommission in Luxemburg betrieben wird, würde jede nationale Anfrage auch zu einer grenzüberschreitenden europäischen Datenübermittlung werden. Problematisch ist es, dass sich die Kommission bislang weigert, den für die Vorabkontrollen bei der Implementation von IMI und dessen innerstaatliche Verwendung zuständigen Datenschutzbeauftragten der Länder das dem Verfahren IMI zugrunde liegende Sicherheitskonzept und die technischen Verfahrensbeschreibungen zugänglich zu machen. Die Kommission will diese Informationen aber nicht zur Verfügung zu stellen, da das System ausschließlich der datenschutzrechtlichen Kontrolle des Europäischen Datenschutzbeauftragten unterliege. Ich werde die Entwicklung weiterhin kritisch beobachten.

9. 22. TB Nr. 10.1 **Gendiagnostikgesetz: Gentests Grenzen gesetzt**

Das am 1. Februar 2010 in Kraft getretene Gendiagnostikgesetz regelt genetische Untersuchungen und Analysen sowie den Umgang mit dabei gewonnenen genetischen Proben. Dabei enthält das Gesetz zahlreiche datenschutzfreundliche Regelungen wie etwa das Recht, die eigenen genetischen Befunde zu kennen, aber auch das Recht, diese nicht zu kennen, wenn man dies nicht möchte.

Wesentliche Bestimmungen betreffen die so genannten Vaterschaftstests, die nur mit Zustimmung der zu untersuchenden Person zulässig sind. Heimliche Abstammungsuntersuchungen dürfen dagegen nicht veranlasst werden. Eine genetische Untersuchung zu medizinischen Zwecken darf nur ein Arzt vornehmen. Erlaubt die Untersuchung eine Vorhersage über die eigene Gesundheit oder die eines ungeborenen Kindes, ist eine genetische Beratung vor oder nach der Untersuchung Pflicht.

Im Arbeitsrecht sind genetische Untersuchungen auf Verlangen des Arbeitgebers grundsätzlich verboten. Lediglich im Rahmen des Arbeitsschutzes können unter eng gefassten Voraussetzungen genetische Untersuchungen zulässig sein.

Versicherungsunternehmen dürfen weder vor noch nach Abschluss des Versicherungsvertrages die Vornahme genetischer Untersuchungen oder die Mitteilung von Ergebnissen aus vorangegangenen genetischen Untersuchungen verlangen. Hiervon gibt es zur Vermeidung von Missbrauchsfällen eng begrenzte Ausnahmen bei Abschlüssen von Lebens-, Berufsunfähigkeits-, Erwerbsunfähigkeits- und Pflegeversicherungen mit einem bestimmten hohen Leistungsumfang.

Bestimmungen, die den datenschutzgerechten Umgang mit genetischen Untersuchungen in der Forschung beinhalten, enthält das Gesetz leider nicht. Dies ist sehr bedauerlich, da gerade in diesem Bereich bei allen Beteiligten eine große Rechtsunsicherheit herrscht.

10. 22. TB Nr. 12.3 **Online-Anbindung der Kfz-Zulassungsstellen an das Kraftfahrt-Bundesamt**

Seit vielen Jahren beschäftige ich mich mit der Online-Anbindung der örtlichen Fahrerlaubnisbehörden an das Kraftfahrt-Bundesamt (KBA). Im Jahr 2010 hat das BMVBS das von mir geforderte Gesetzgebungsverfahren auf den Weg gebracht. Im Rahmen der Ressortabstimmung habe ich eine Vielzahl von Änderungen empfohlen. So habe ich gefordert, im StVG normenklare Regelungen zu den Protokollierungspflichten des KBA bzw. der örtlichen Fahrerlaubnisbehörden zu treffen und die Revisionssicherheit des Zentralen Fahrerlaubnisregisters (ZFER) zu gewährleisten. Allerdings wurde keine meiner datenschutzrechtlichen Empfehlungen vom BMVBS angenommen. Die entsprechenden Regelungen im Gesetz zur Änderung des Straßenverkehrsgesetzes sind zum 3. Dezember 2010 in Kraft getreten (BGBl I 2010 S. 1748).

Ich bedauere, dass das BMVBS meine Vorschläge nicht aufgegriffen hat. Die neuen gesetzlichen Regelungen der §§ 51 ff. StVG weisen immer noch die bekannten Unzulänglichkeiten auf. So klaffen weiterhin gesetzliche Vorgaben und Realität auseinander, insbesondere mit Blick auf die Tatsache, dass die örtlichen Fahrerlaubnisbehörden direkt und unmittelbar auf den Datenbestand des ZFER ändernd zugreifen und somit auch die volle Verantwortung für die Richtigkeit der gespeicherten Daten haben. Ebenso bleibt es bei den unklaren Vorgaben zu den Protokollierungspflichten der Fahrerlaubnisbehörden und des KBA. Die Chance, das ZFER als Verbunddatei zu definieren, klare Verantwortlichkeiten festzulegen und dadurch auch die Revisionssicherheit dieses Registers zu gewährleisten, wurde nicht genutzt. Ebenfalls sehr bedauerlich ist, dass die korrespondierenden Reglungen in der Fahrerlaubnisverordnung noch nicht angepasst sind.

11. 22. TB Nr. 4.2.1 **Bündelung der Telekommunikationsüberwachung beim Bundesverwaltungsamt**

Ich hatte über Pläne des BMI berichtet, Einrichtungen zur Telekommunikationsüberwachung durch Polizei und Nachrichtendienste des Bundes und der Länder beim Bundesverwaltungsamt (BVA) zusammenzufassen.

Hiervon rückte das BMI im Februar 2010 insofern ab, als die Einrichtungen zur Telekommunikationsüberwachung nicht mehr auf die Verfassungsschutzbehörden ausgedehnt werden sollten. Nur Telekommunikationsüberwachungsmaßnahmen durch BKA und Bundespolizei sollten weiterhin im Bundesverwaltungsamt gebündelt werden. Eine Rechtsgrundlage sei hierfür nicht mehr erforderlich, da es sich um eine Auftragsdatenverarbeitung gem. § 11 BDSG durch das BVA handele.

Zwar begrüße ich die Entscheidung des BMI, von einer Einbeziehung der Verfassungsschutzbehörden abzusehen. Eine umfassende Zusammenlegung der Telekommunikationsüberwachung der verschiedenen Si-

cherheitsbehörden hätte die Grenzen zwischen Polizei und Nachrichtendiensten verwischt und das Trennungsgebot verletzt. Gleichwohl halte ich eine gesetzliche Regelung für die Durchführung von Telekommunikationsüberwachungsmaßnahmen für BKA und Bundespolizei durch das BVA weiterhin für erforderlich. Es handelt sich hierbei um eine in besonderer Weise sensible Behördenkooperation, die erheblich in das vom Grundgesetz geschützte Fernmeldegeheimnis eingreift.

12. 22. TB Nr. 5.2 und 6.5 **Bundesmeldegesetz**

Aufgrund der von mir im Jahre 2008 geäußerten Bedenken zum Referentenentwurf eines Bundesmeldegesetzes hat das BMI seine Überlegungen vorgestellt, das ursprünglich vorgesehene umfängliche Bundesmelderegister durch ein schlankeres sog. Einwohnerinformationssystem auf Bundesebene zu ersetzen. Doch auch den hier vorzufindenden Merkmalskatalog habe ich mit Blick auf den Bedarf einer zentralen Datenspeicherung auf Bundesebene als zu umfangreich bewertet. BMI hat in der 16. Legislaturperiode auf die erneute Vorlage eines Referentenentwurfs verzichtet. Inzwischen besteht in der Bundesregierung offenbar Einigkeit darüber, auf ein zentrales Melderegister ganz zu verzichten. Ob in der laufenden 17. Legislaturperiode ein neuer Entwurf vorgelegt wird, bleibt abzuwarten.

## Anlagen

**Anlage 1**

**Hinweis für die Ausschüsse des Deutschen Bundestages**

Nachfolgend habe ich dargestellt, welche Beiträge dieses Berichtes für welchen Ausschuss von *besonderem Interesse* sein könnten:

| | |
|---|---|
| Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung | |
| Auswärtiger Ausschuss | 5.6, 5.9, 5.11; 13.7; 13.12, 13.13, 13.14; 15.1; 15.4 |
| Innenausschuss | 1.1 bis 1.6; 2.1 bis 2.7, 3, 3.1; 3.2; 3.3; 3.5; 4.1, 4.1.1 bis 4.1.4, 4.2, 4.3 bis 4.6; 4.8, 4.9; 4.10; 5.2, 5.3, 5.4, 5.4.2, 5.5, 5.7, 5.10, 5.11; 5.12, 5.13, 6.1 bis 6.10; 7.1.1, 7.1.2, 7.1.5 bis 7.1.7, 7.2.2, 7.2.3, 7.3.1, 7.3.2, 7.5.1, 7.7; 8.1.1; 8.1.2; 8.2.1; 8.3, 8.4, 8.6; 8.8; 9.8; 10.5 bis 10.7; 12.3 bis 12.5; 13.1, 13.2; 13.5 bis 13.10, 13.11.1; 14.2, 14.3; 15.1; 15.8; 15.9; 15.12 |
| Sportausschuss | 8.7 |
| Rechtsausschuss | 1.1 bis 1.6; 2.1 bis 2.7; 4.1, 4.1.1 bis 4.1.4, 4.2, 4.3 bis 4.6; 4.8, 4.9; 5.2, 5.12, 5.13; 6.1 bis 6.10; 7.1.1, 7.1.2, 7.1.5, 7.1.7, 7.2.3, 7.3.2, 7.5.1; 8.1.2; 8.10; 9.1; 9.8; 10.5 bis 10.7; 13.1, 13.2; 13.5 bis 13.10 |
| Finanzausschuss | 3.6; 9.1 bis 9.5 |
| Ausschuss für Wirtschaft und Technologie | 1.3, 1.5, 1.6; 3, 3.1 bis 3.4; 4.1.3, 4.1.4, 4.3 bis 4.6; 4.8; 5.1 bis 5.6, 5.8, 5.9, 5.10, 5.12; 6.1 bis 6.10; 6.12; 7.7; 9.8; 10.2, 10.5 bis 10.8; 15.8, 15.9, 15.10 |
| Ausschuss für Ernährung, Landwirtschaft und Verbraucherschutz | 1; 3, 3.3; 4.1, 4.1.1 bis 4.1.3, 4.2, 4.3, 4.5; 5.3, 5.6, 5.9, 5.10, 5.11, 10.3, 10.5 bis 10.7 |
| Ausschuss für Arbeit und Soziales | 3, 3.1, 3.3; 5.4.2, 5.5; 11.1.2, 11.1.3, 11.1.8, 11.1.9, 11.2; 11.5.1, 11.5.2, 12.1 |
| Verteidigungsausschuss | |
| Ausschuss für Familie, Senioren, Frauen und Jugend | 11.2 |
| Ausschuss für Gesundheit | 3; 4.3.1; 5.4.1; 11.1.1, 11.1.4 bis 11.1.8, 11.1.10, 11.3; 11.4; 15.5, 15.6, 15.7, 15.9 |
| Ausschuss für Verkehr, Bau und Stadtentwicklung | 5.1, 5.4.2, 5.8, 10.8, 10.9; 12.2, 12.4 |
| Ausschuss für Menschenrechte und Humanitäre Hilfe | |
| Ausschuss für Bildung, Forschung und Technikfolgenabschätzung | 1.2, 1.3, 1.5, 1.6; 3; 5.3, 5.6, 5.9, 5.10, 5.11, 5.12; 8.7; 11.3 |
| Ausschuss für Tourismus | |
| Ausschuss für die Angelegenheiten der Europäischen Union | 3.1; 5.9; 13.1, 13.2; 13.5 bis 13.10; 13.12; 15.8 |
| Ausschuss für Kultur und Medien | 4.3 bis 4.6; 6.1; 8.5 |
| Ausschuss für Kultur und Medien – Unterausschuss „Neue Medien“ – | 1.2, 1.3, 1.5, 1.6; 3, 3.1, 3.3, 3.5; 4.3 bis 4.6; 5.2, 5.3, 5.4, 5.6, 5.9, 5.10, 5.11, 5.12; 7.1.7 |

**Anlage 2**

**Übersicht über die durchgeführten Kontrollen, Beratungen und Informationsbesuche**

**Bundeskanzleramt (einschließlich Beauftragter für Kultur und Medien)**

- Bundesnachrichtendienst
- Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (Zentrale und zwei Außenstellen)

**Bundesministerium des Innern**

- Ministerium
- Ausländerzentralregister
- Bundesverwaltungsamt
- Bundesverwaltungsamt (Register der Entscheidungen in Staatsangehörigkeitsangelegenheiten)
- Bundesamt für Verfassungsschutz
- Bundeskriminalamt (Wiesbaden, Meckenheim, Berlin)
- Bundespolizeidirektion Flughafen Frankfurt/Main
- Forschungs- und Erprobungsstelle der Bundespolizei, Lübeck
- Technisches Hilfswerk
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

**Bundesministerium der Justiz**

- Bundesamt für Justiz
- Deutsches Patent- und Markenamt

**Bundesministerium der Finanzen**

- Ministerium (ELSTER-Online)
- Bundesanstalt für Finanzdienstleistungsaufsicht
- Zollkriminalamt

**Bundesministerium für Arbeit und Soziales**

- Deutsche Rentenversicherung Bund
- Bundesagentur für Arbeit
- Zentrale Auslands- und Fachvermittlung
- Familienkasse der Bundesagentur für Arbeit
- Jobbörse

**Bundesministerium der Verteidigung**

- Militärischer Abschirmdienst

**Bundesministerium für Gesundheit**

- Ministerium
- Paul-Ehrlich-Institut
- GKV Spitzenverband
- Bundesversicherungsamt

**Bundesministerium für Verkehr, Bau und Stadtentwicklung**

- Ministerium
- Bundesamt für Seeschifffahrt und Hydrographie
- Wasser- und Schifffahrtsamt Hamburg
- Eisenbahnbundesamt

**Bundesministerium für Wirtschaft und Technologie**

- Bundesamt für Wirtschaft und Ausfuhrkontrolle

**Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz**

- Max-Rubner-Institut

**Deutsche Post AG**

- Zentrale
- Rechenzentrum Ratingen
- Druckzentrum Kleinmachnow

**Telekommunikationsunternehmen**

- MyPhone GmbH
- Vodafone D2 GmbH
- E-Plus Mobilfunk GmbH & Co. KG
- blau Mobilfunk GmbH
- Deutsche Telekom AG
- Communication Services Tele2 GmbH

**Sonstige**

- DPD Dynamic Parcel Distribution GmbH & Co. KG
- Hermes Europe GmbH
- Toll Collect GmbH
- Value 5
- BARMER Ersatzkasse
- BKK Gesundheit
- IKK Signal Iduna
- Wirtschaftsunternehmen wegen Verfahren zur Sicherheitsüberprüfung im Rahmen des vorbeugenden personellen Sabotageschutzes

**Anlage 3**

## Übersicht über Beanstandungen nach § 25 BDSG

### Bundesministerium des Innern

– Verstoß des Ausländerzentralregisters (AZR) gegen § 9 Satz 1 BDSG einschließlich Anlage, da mit Blick auf das automatisierte Abrufverfahren nach § 22 AZR-Gesetz die Vorgaben des Europäischen Gerichtshofs in der Rechtssache Huber zum Schutz der im AZR gespeicherten personenbezogenen Daten von Unionsbürgern (Urteil vom 16.12.2008, Rs. C-524/06) nicht durch entsprechende technisch-organisatorische Maßnahmen umgesetzt wurden (vgl. Nr. 8.2.1).

### Bundesministerium der Finanzen

– Verstoß gegen § 19 Absatz 1 BDSG, indem durch eine Dienstanweisung vom 17. Dezember 2008 (IV A 3 – S 0030/08/10001) die Gewährung des Auskunftsrechts der Steuerpflichtigen von dem Nachweis eines berechtigten Interesses abhängig gemacht wird (vgl. Nr. 9.4).

– Verstoß des Bundeszentralamtes für Steuern (BZSt) gegen § 9 Satz 1 BDSG einschließlich Anlage, da die beim BZSt eingerichtete Datenbank zur Steuer-Identifikationsnummer in Betrieb genommen wurde, ohne dass ein vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorlag.

### Bundesministerium für Verkehr, Bau und Stadtentwicklung

20 Beanstandungen (vgl. Nr. 12.2)

– fünf Verstöße gegen § 90 Absatz 1 und 4 BBG a. F. und gegen § 90g BBG a. F.,

– Verstoß gegen § 90 Absatz 1 Satz 1 und Absatz 3 BBG a. F. und § 90g BBG a. F. (vgl. 12.2),

– vier Verstöße gegen das Fernmeldegeheimnis nach § 88 TKG,

– Verstoß gegen §§ 75, 80 Absatz 1 Nummer 1, Absatz 2 Satz 1 und § 87 Absatz 1 Nummer 6 BetrVG,

– Verstoß gegen § 87 Absatz 1 Nummer 6 BetrVG,

– zwei Verstöße gegen § 4 Absatz 1 BDSG, § 90 Absatz 1 und 4 BBG a. F. und § 90g BBG a. F.,

– zwei Verstöße gegen § 4 Absatz 1 BDSG,

– Verstoß gegen § 4g Absatz 1 Satz 1 BDSG,

– Verstoß gegen § 4e Nummer 4 und 6 BDSG,

– Verstoß gegen § 4d Absatz 5 BDSG,

– Verstoß gegen § 9 sowie Anlage zu § 9 Satz 1 BDSG.

### Bundesministerium für Wirtschaft und Technologie

– Verstoß des Bundesamtes für Wirtschaft und Ausfuhrkontrolle gegen § 9 BDSG (fehlende Verschlüsselung)

– und gegen § 4g Absatz 1 Nummer 1 BDSG (fehlende bzw. nicht rechtzeitige Einbeziehung des behördlichen Datenschutzbeauftragten)

jeweils bei der Online-Beantragung der Umweltprämie (Nr. 10.2)

### Telekommunikationsunternehmen

### Deutsche Telekom AG

– Verstoß gegen § 4g Absatz 1 und 2 BDSG wegen unzureichender Einbindung des behördlichen Datenschutzbeauftragten (s. Nummer 6.3)

### Gesetzliche Krankenkassen

Vier Beanstandungen (vgl. Nummer 11.1.4)

– Verstoß gegen § 81 Absatz 4 SGB X i. V. mit § 4f Absatz 5 Satz 1, § 4g Absatz 2 Satz 1 BDSG,

– Verstoß gegen § 67b Absatz 1 SGB X,

– Verstoß gegen die Bestimmungen der § 80 Absatz 2 Satz 1, § 67a Absatz 1 Satz 1 und Satz 2 SGB X i. V. m. § 78a SGB X und der Anlage zu § 78a SGB X,

– Verstoß gegen § 80 SGB X a. F. i. V. mit § 78a SGB X und der Anlage zu § 78a SGB X.

**Anlage 4**

**Deutscher Bundestag** **Drucksache 16/12271**

**16. Wahlperiode** 17. 03. 2009

# Beschlussempfehlung und Bericht

## des Innenausschusses (4. Ausschuss)

## zu der Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – Drucksache 16/4950 –

## Tätigkeitsbericht 2005 und 2006 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – 21. Tätigkeitsbericht –

### A. Problem

Der 21. Tätigkeitsbericht stellt die Arbeitsschwerpunkte des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in den Jahren 2005 und 2006 überblickartig dar und geht dabei insbesondere auf die zunehmenden, technologisch bedingten Kontroll- und Überwachungsrisiken sowohl im Verhältnis Staat/Bürger als auch beim Umgang der Wirtschaft mit personenbezogenen Daten ein. Schwerpunkte setzt der Bericht unter anderem bei der Darstellung und Beurteilung europäischer Rechtsentwicklungen, beim technologischen Datenschutz und bei datenschutzrechtlichen Fragen der inneren Sicherheit. Dabei werden auch wichtige Feststellungen zur datenschutzrechtlichen Kontrolle von öffentlichen Stellen des Bundes getroffen. Zentrale Bedeutung für die weitere Entwicklung zur Informationsgesellschaft misst der Bericht der Frage bei, wie der Gesetzgeber zukünftig von seinen Gestaltungsoptionen Gebrauch mache, ob er die Grundrechtspositionen stärke oder neue Grundrechtseinschränkungen legitimiere.

### B. Lösung

Kenntnisnahme der Unterrichtung und einstimmige Annahme einer Entschließung

### C. Alternativen

Keine

### D. Kosten

Keine

noch Anlage 4

**Beschlussempfehlung**

Der Bundestag wolle beschließen, in Kenntnis der Unterrichtung auf Drucksache 16/4950 folgende Entschließung anzunehmen:

| | | |
|---|---|---|
| 1. | Der Deutsche Bundestag begrüßt, dass die Bundesregierung seine Forderung aus den Entschließungen zum 19. und 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Vorlage eines Datenschutzauditgesetzes gemäß § 9a BDSG aufgegriffen hat und an einem entsprechenden Gesetzentwurf arbeitet. Ein solches Gesetz muss den Unternehmen die Möglichkeit eines Audits auf freiwilliger Basis bieten und unbürokratisch ausgestaltet sein.<br><br>Dieses Projekt muss jetzt zügig vorangebracht werden, damit ein Datenschutzauditgesetz noch in dieser Legislaturperiode verabschiedet werden kann (21. TB, Nr. 2.4). | **Nicht erledigt**<br><br>vgl. Nr. 2.2 |
| 2. | Der Abstand zwischen den geltenden datenschutzrechtlichen Bestimmungen und der rasanten technologischen Entwicklung mit ihren Folgen in allen Lebensbereichen wird immer größer. Das vom Deutschen Bundestag geforderte moderne, leicht verständliche und übersichtliche Datenschutzrecht wäre nicht nur ein wirtschaftlicher Standortvorteil, sondern könnte auch einen wertvollen Beitrag zur Entbürokratisierung leisten (21. TB, Nr. 2.1). | **Nicht erledigt**<br><br>vgl. Kapitel 1 |
| 3. | Der Deutsche Bundestag beobachtet sorgfältig die Entwicklung von Informations- und Kommunikationstechnologien, die neben Vorteilen für das tägliche Leben auch neue Risiken wie z. B. Identitätsdiebstahl, diskriminierende Profilerstellung oder Betrugsdelikte mit sich bringen.<br><br>Die Bundesregierung wird aufgefordert, dafür Sorge zu tragen, dass datenschutzfreundliche Technologien weiter entwickelt, verbreitet und verwendet werden, um den Schutz der Privatsphäre und den Datenschutz zu verbessern. | **Nicht erledigt**<br><br>vgl. Nr. 3 |
| 4. | Nachdem auf europäischer Ebene eine Initiative zum Arbeitnehmerdatenschutz nicht mehr zu erwarten ist, weist der Deutsche Bundestag die Bundesregierung noch einmal nachdrücklich auf seine mehrfach erhobene Forderung hin, schnellstmöglich einen Gesetzentwurf zum Arbeitnehmerdatenschutz vorzulegen (21. TB, Nr. 2.7). | **Ist dabei, erledigt zu werden**<br><br>vgl. Nr. 12.1 |
| 5. | Der Deutsche Bundestag hat zuletzt in seiner Entschließung zum 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Bundesregierung an ihre Zusage erinnert, den Betroffenen auch gegenüber der Steuerverwaltung einen Anspruch auf Auskunft zu den über sie gespeicherten Daten einzuräumen. Gleichzeitig hatte er die Bundesregierung aufgefordert, ihre Prüfungen über die personellen, organisatorischen und haushalterischen Auswirkungen eines solchen Auskunftsanspruchs zeitnah abzuschließen.<br><br>Dieser Aufforderung ist die Bundesregierung noch immer nicht nachgekommen. Der Deutsche Bundestag fordert die Bundesregierung deshalb erneut auf, den Auskunftsanspruch des Betroffen auch in der Steuerverwaltung sicherzustellen. | **Noch nicht erledigt**<br><br>Das Bundesministerium der Finanzen hat einen Diskussionsentwurf zur Schaffung einer gesetzlichen Regelung zum Auskunftsanspruch vorgelegt, der derzeit erörtert wird.<br><br>vgl. 23. TB Nr. 9.4 |
| 6. | Der Deutsche Bundestag fordert die Bundesregierung auf, die Bürgerinnen und Bürger besser vor den Gefahren des Missbrauchs biometrischer Systeme zu schützen. Bei der Entwicklung von Biometrieanwendungen muss ein hoher Datenschutzstandard gewährleistet sein, so dass der Datenschutz der Bürgerinnen und Bürger sichergestellt ist und Missbrauchsmöglichkeiten ausgeschlossen sind. | **Nur in einigen Punkten erledigt, überwiegend nicht**<br><br>vgl. u. a. Nr. 3.5 |

noch Anlage 4

| | | |
|---|---|---|
| 7. | Der Deutsche Bundestag teilt die Auffassung der Bundesregierung, dass das Bundesdatenschutzgesetz auch für Rechtsanwälte gilt. Er begrüßt, dass die Bundesregierung prüft, welche gesetzlichen Regelungen sich im Zusammenhang mit der Verarbeitung mandatsbezogener Daten durch Rechtsanwälte empfehlen, um eine wirksame Datenschutzkontrolle zu gewährleisten, ohne dass das besonders geschützte Vertrauensverhältnis zwischen Rechtsanwalt und Mandant in unzulässiger Weise beeinträchtigt wird. | **Nicht erledigt** |

In der Plenarsitzung des Deutschen Bundestages vom 19. März 2009 einstimmig angenommen.

**Anlage 5**

**Deutscher Bundestag** **Drucksache 17/4179**

**17. Wahlperiode** 14.12.2010

# Beschlussempfehlung und Bericht

## des Innenausschusses (4. Ausschuss)

## zu der Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – Drucksache 16/12600, 17/790 Nr. 5 –

## Tätigkeitsbericht 2007 und 2008 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – 22. Tätigkeitsbericht –

### A. Problem

Der 22. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit stellt die Arbeitsschwerpunkte einschließlich der Kontrollergebnisse öffentlicher Stellen in den Jahren 2007 und 2008 überblicksartig dar. Eine grundlegende Modernisierung des Datenschutzrechts wird angemahnt. Der Datenschutz in der Privatwirtschaft einschließlich des Beschäftigtendatenschutzes wird umfassend problematisiert. Weitere Schwerpunkte setzt der Bericht bei gesetzgeberischen Maßnahmen im Bereich der inneren Sicherheit, der internationalen Rechtsentwicklung, dem technologischen Datenschutz und dem Datenschutz im Internet. Der Umgang mit Geodaten eröffnet dabei eine neue Dimension von Datenschutzfragen.

### B. Lösung

Einstimmige Annahme einer Entschließung Kenntnisnahme der Unterrichtung.

### C. Alternativen

Keine

### D. Kosten

Keine

noch Anlage 5

**Beschlussempfehlung**

Der Bundestag wolle beschließen, in Kenntnis der Unterrichtung auf Drucksache 16/12600 folgende Entschließung anzunehmen:

„1. Der Deutsche Bundestag hat schon mehrfach die große Bedeutung eines präventiven technologischen Datenschutzes unterstrichen. Neue Technologien haben bereits bei ihrer Entwicklung wie auch bei ihrem Einsatz den Erfordernissen eines wirksamen Datenschutzes zu entsprechen. Gesetzliche Vorgaben sollten verpflichtend und technikneutral die Schutzziele bestimmen, damit der Datenschutz auch bei weiterem technologischem Fortschritt gewährleistet und bereits im Entwicklungsstadium von neuen Produkten und Geschäftsmodellen berücksichtigt wird.

2. Der Deutsche Bundestag sieht mit Sorge, wie es die Vielzahl der Datenverarbeitungen und das unaufhörliche Anwachsen von Datenbeständen den Bürgerinnen und Bürgern immer schwerer macht, ihr informationelles Selbstbestimmungsrecht auch tatsächlich auszuüben. Eine Stärkung der Betroffenenrechte ist deswegen dringend geboten.

   Eine engere Zweckbindung in den gesetzlichen Normen stärkt die Selbstbestimmung der Betroffenen über den Umgang mit ihren persönlichen Daten und begegnet der zunehmenden Vernetzung unterschiedlicher Datenbestände, die auch vom Bundesverfassungsgericht als große Gefahr für das Persönlichkeitsrecht gesehen wird. Eine Profilbildung, die ein besonderes Gefährdungspotenzial in sich birgt, ist nur dann zulässig, wenn sie durch eine entsprechende gesetzliche Grundlage erlaubt ist oder der Betroffene wirksam eingewilligt hat. Außerdem muss die Sammlung personenbezogener Daten ohne Kenntnis der Betroffenen wieder zur Ausnahme werden.

   Die verantwortlichen Stellen müssen grundsätzlich zu einer umfassenden Information der Betroffenen verpflichtet werden. Außerdem müssen die Rechte auf Auskunft, Löschung, Sperrung oder Widerspruch in ihrer Ausübung und Durchsetzung bürgerfreundlicher werden und auch im Kontext des Internet einfach handhabbar und realisierbar sein.

   Dabei kommt dem Einsatz moderner Technologien (etwa dem Recht auf Auskunft über die gespeicherten Daten und einem Widerspruchsrecht, deren Ausübung auch auf elektronischem Wege zu ermöglichen ist) besondere Bedeutung zu. Die Bundesregierung wird aufgefordert, entsprechende Vorschläge zu erarbeiten.

3. Der Deutsche Bundestag beobachtet sorgfältig die besondere Gefährdung des Grundrechts auf informationelle Selbstbestimmung, die sich aus neuen technischen Möglichkeiten und einem veränderten Kommunikationsverhalten ergeben, insbesondere im Zusammenhang mit der Weiterentwicklung des Internet. Er begrüßt es daher, dass sich auch die Bundesregierung dieser Thematik verstärkt zugewandt hat.

   Neben flankierenden gesetzlichen Regelungen können Selbstverpflichtungen der beteiligten Branchen das Datenschutzniveau verbessern.

4. Für wirkungsvollen Datenschutz, insbesondere im Internet, ist es unerlässlich, dass auch die Betroffenen selbst verantwortungsvoll mit ihren personenbezogenen Daten umgehen und die Möglichkeiten technischer Schutzmaßnahmen nutzen. Hierfür fehlt es aber noch immer an der erforderlichen Sensibilität für mögliche Gefahren und an Wissen darüber, welche Maßnahmen des Selbstschutzes möglich und sinnvoll sind.

   Aufklärung und entsprechendes technisches Knowhow sind deswegen wichtige datenschutzpolitische Ziele. Der Deutsche Bundestag fordert die Bundesregierung auf, sich diesen Aufgaben verstärkt zu widmen, z. B. durch Errichtung der Stiftung Datenschutz.

   Dabei hat die Bundesregierung dafür Sorge zu tragen, dass keine Parallelstrukturen oder Konkurrenz zu den durch die Datenschutzbeauftragten des Bundes und der Länder wahrgenommenen Aufgaben entstehen.

5. Kinder und Jugendliche können vielfach die mit der Nutzung moderner Techniken verbundenen Konsequenzen und Risiken nicht erkennen oder richtig einschätzen. Ein verstärktes Bemühen um Aufklärung und Bildung im Bereich Datenschutz ist vor diesem Hintergrund gerade auch bei jungen Menschen geboten.

   Hierzu soll die geplante Stiftung Datenschutz einen wesentlichen Beitrag leisten, ohne mit den bereits bestehenden Angeboten in Konkurrenz zu treten. Der Deutsche Bundestag begrüßt in diesem Zusammenhang die Bildungsinitiativen der Datenschutzbeauftragten des Bundes und der Länder.

   Der Deutsche Bundestag fordert die Bundesregierung auf zu prüfen, wie neben dieser Bereitstellung von Bildungsangeboten auch durch gesetzliche Vorgaben der Datenschutz insbesondere von Kindern und Jugendlichen verbessert werden kann.

6. Der Bundestag begrüßt das Eckpunktepapier der Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Ein modernes Datenschutzrecht für das 21. Jahrhundert“.

Er fordert die Bundesregierung auf, Möglichkeiten zur Umsetzung der dort gemachten Vorschläge und Anreize zu prüfen und darüber hinaus die Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihre politischen und gesetzgeberischen Überlegungen mit einfließen zu lassen.

7. Datenschutzgütesiegel und Datenschutzaudits können im Verhältnis zwischen Bürgern, Unternehmen und Staat ein wesentliches Instrument zur Vertrauensbildung darstellen. Sie sind geeignet, die Eigenverantwortlichkeit der verantwortlichen Stelle zu fördern und zu stärken. Der Deutsche Bundestag bedauert es daher, dass auch in der 16. Wahlperiode keine Verständigung über ein einheitliches und bundesweit anerkanntes Zertifizierungsinstrument erfolgen konnte. Insofern begrüßt er das Vorhaben der Bundesregierung eine Stiftung Datenschutz errichten zu wollen, die diesen Missstand aufgreifen und Vorschläge für eine transparente Zertifizierungspraxis erarbeiten soll. Der Deutsche Bundestag weist in diesem Zusammenhang darauf hin, dass die Stiftung Datenschutz jedoch nur dann den gewünschten Erfolg erzielen wird, wenn sowohl in personeller, als auch in wirtschaftlicher Hinsicht ihre Unabhängigkeit gewährleistet ist.

8. Mit Interesse hat der Deutsche Bundestag das Urteil des Europäischen Gerichtshofes zur Unabhängigkeit der Datenschutzaufsichtsbehörden in den Ländern zur Kenntnis genommen. Der Bundestag fordert die Bundesregierung auf zu prüfen, ob durch die Entscheidung auch auf Bundesebene ein gesetzgeberisches Handeln erforderlich ist.

   Bei einer Neuregelung sollten Eingriffsmöglichkeiten und Rechtsrahmen der Datenschutzaufsicht möglichst einheitlich ausgestaltet und die Effizienz des Datenschutzes gewährleistet werden.

   Zudem regt der Deutsche Bundestag an zu prüfen, ob der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit im Bereich der seiner Aufsichtszuständigkeit unterliegenden Post- und Telekommunikationsdienstleistungen die gleichen nach § 38 BDSG definierten Handlungs- und Sanktionsmöglichkeiten wie die Aufsichtsbehörden der Länder erhalten sollte.

9. Der Deutsche Bundestag fordert die Bundesregierung dazu auf, sich in den bevorstehenden Verhandlungen zur Novellierung der EU-Datenschutzrichtlinie 95/46 vom 23.11.1995 für die Sicherung eines hohen Datenschutzniveaus entsprechend der bundesdeutschen Datenschutzbestimmungen einzusetzen. Er bittet zudem die Bundesregierung zu prüfen, inwiefern die Modernisierungsvorschläge der Datenschutzbeauftragten des Bundes und der Länder hierbei Berücksichtigung finden können.

10. Der Deutsche Bundestag beobachtet sorgfältig die ständig fortschreitende globale Vernetzung, die allein durch nationale Datenschutzgesetze nicht geregelt werden kann. Deshalb müssen internationale Instrumente entwickelt werden, welche den Schutz der Persönlichkeitsrechte der Betroffenen wirksam gewährleisten. Der Deutsche Bundestag begrüßt daher die Absicht der EU, in einem allgemeinen Datenschutzabkommen für die polizeiliche und justizielle Zusammenarbeit mit den Vereinigten Staaten von Amerika hierfür die Voraussetzungen zu schaffen. Dabei müssen aber die europaweit und national geltenden Datenschutzstandards eingehalten und fortgeschrieben werden.

11. Der Deutsche Bundestag hat bereits in seiner Entschließung zum 20. Tätigkeitsbericht des BfDI zur Übermittlung von Fluggastdaten in die USA Stellung genommen (BT-Drucks. 16/4882, Nr. 6). Seitdem werden Passagierdaten auch in weitere Staaten übermittelt. Der Deutsche Bundestag ruft die Bundesregierung auf, sich bei der Europäischen Union für die Entwicklung eines Musterabkommens für Fluggastdaten einzusetzen, das hohen Datenschutzstandards genügt und einen angemessenen Rechtsschutz ermöglicht. Ein entsprechendes Abkommen sollte insbesondere Zurückhaltung im Bezug auf den Umfang der zu übermittelnden Daten und deren Speicherdauer üben und auf eine strenge Zweckbindung Wert legen.

12. Staatliche Stellen nutzen zunehmend die ihnen eingeräumte Befugnis, sich im Kontenabrufverfahren über die von Bürgerinnen und Bürgern eingerichteten Konten zu informieren. Der Deutsche Bundestag erinnert daran, dass es sich hierbei um Eingriffe in die Persönlichkeitsrechte der Betroffenen handelt, bei denen der Grundsatz der Verhältnismäßigkeit zu beachten ist. Er fordert die Bundesregierung auf, schnellstmöglich den Prüfauftrag aus dem Koalitionsvertrag umzusetzen und nach Auswertung der Ergebnisse der stetigen Ausweitung der Abfragen durch wirksame Maßnahmen zu begegnen.

13. Der Deutsche Bundestag ist sich der datenschutzrechtlichen Vorbehalte bewusst, die bei vielen Bürgerinnen und Bürgern hinsichtlich der Volkszählung 2011 bestehen.

    Gerade deswegen ist eine datenschutzkonforme Durchführung des Zensus unabdingbar. Dies gilt insbesondere für die Verwendung von Ordnungsnummern, die Gestaltung der Fragebögen und die Durchführung der Zählung in sensiblen Sonderbereichen.

14. Bei der anstehenden Reform des Melderechts sieht der Deutsche Bundestag keine Notwendigkeit für eine zentrale Speicherung. In jedem Fall muss das Melderecht grundsätzlich auf seine Kernfunktionen beschränkt werden.

    Die bisherige Praxis der listenmäßigen Übermittlung von Einwohnerdaten an Dritte sollte überprüft werden.

noch Anlage 5

15. Der Deutsche Bundestag bedauert, dass seine Aufforderung aus den Entschließungen zum 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BT-Drucks. 16/4882, Nr. 10) und zum 21. Tätigkeitsbericht (BT-Drucks. 16/12271, Nr. 5), auch für die Steuerverwaltung den datenschutzrechtlichen Auskunftsanspruch gesetzlich festzuschreiben, noch zu keinem Ergebnis geführt hat. Er hält an seiner Forderung fest, die Abgabenordnung um einen entsprechenden vorbehaltlosen gesetzlichen Anspruch zu erweitern.

16. Die Möglichkeit, mithilfe intelligenter Stromzähler den tatsächlichen Stromverbrauch kontrollieren zu können, könnte einen ökonomischen Mehrwert für den Verbraucher schaffen und beträchtliche ökologische Vorteile mit sich bringen. Bei ihrem Betrieb fallen jedoch auch umfangreiche und differenzierte Datenbestände (Lastprofile) an, die durch geeignete technische und organisatorische Maßnahmen wirksam vor dem Zugriff durch Unberechtigte geschützt werden müssen. Auch muss sichergestellt werden, dass die Datenhoheit beim Verbraucher verbleibt und dieser selbst darüber entscheiden kann, welche Daten er zur Verfügung stellen möchte.

    Der Bundestag fordert daher die Bundesregierung auf, ihn bei dem Anliegen, neue Technologien datenschutzkonform ausgestalten zu wollen, auch in Zukunft zu unterstützen und die Notwendigkeit der Schaffung gesetzlicher Vorgaben in diesem Bereich zu prüfen.“

In der Plenarsitzung des Deutschen Bundestages vom 18. Dezember 2010 einstimmig angenommen.

**Anlage 6**

Konferenz der Datenschutzbeauftragten
des Bundes und der Länder

# Ein modernes Datenschutzrecht für das 21. Jahrhundert

Eckpunkte

verabschiedet von der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder am 18. März 2010

noch Anlage 6

**Inhaltsverzeichnis**

noch Anlage 6



# Vorwort

Heute ist es nahezu selbstverständlich, jederzeit und aller Orten erreichbar zu sein. Videokameras, die für Sicherheit sorgen sollen, sind ebenso selbstverständlich wie elektronische Helfer in allen Lebenslagen, z. B. Navigationshilfen und elektronische Sensoren, die die Temperatur in Wohn- und Arbeitsräumen regulieren. Diese Entwicklung hin zur allgegenwärtigen Datenverarbeitung hat aber auch ihre Kehrseite: Wir sind nie mehr wirklich allein und können unseren „Datenschatten“ nicht abschütteln, wir haben zudem kaum eine Möglichkeit, diesen überhaupt zu bemerken. Ob von staatlichen Stellen oder Unternehmen – unser Verhalten wird beobachtet, registriert und bewertet. Videoüberwachung folgt uns an allen möglichen Orten, wir können durch Ortungstechnik metergenau lokalisiert werden, Kundenkarten und Internet liefern die Daten für Konsum- und Persönlichkeitsprofile und Auskunfteien haben ein waches Auge auf unsere Zahlungsfähigkeit. Wie soll das Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen Datenverarbeitung ausgestaltet sein? Das heutige Datenschutzrecht gibt hierauf nur noch unbefriedigende Antworten und bedarf der Modernisierung. Datenschutz hat nicht nur eine Schutzfunktion, er beschreibt auch einen Gestaltungsanspruch der Betroffenen: Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Datenschutz ist Grundrechtsschutz und die Wahrung der informationellen Selbstbestimmung eine Funktionsbedingung einer menschenwürdigen Informationsgesellschaft. Als Grundlage einer Diskussion über eine Reform des Datenschutzrechts und als Grundlage für die Fortführung der Diskussion über grundrechtlich verbürgten Datenschutz legt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die nachfolgenden Eckpunkte vor. Bewusst enthält das Papier nur Eckpunkte, die keinen Anspruch auf Vollständigkeit erheben.

noch Anlage 6

Konferenz der Datenschutzbeauftragten des Bundes und der Länder
„Ein modernes Datenschutzrecht für das 21. Jahrhundert“

2

# 1. Zusammenfassung

*Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Doch wie soll dieses Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen, oftmals unbemerkten Datenverarbeitung gewährleistet werden? Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Eckpunkte formuliert, die Grundlage einer Diskussion über eine Reform des Datenschutzrechts sein sollen.*

**Konkrete Schutzziele und Grundsätze verankern**

Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sollten als allgemeingültige datenschutzrechtliche Grundregelungen einen verbindlichen Mindeststandard festlegen. Sie sollten allgemeine Vorgaben enthalten, die als Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nicht-öffentliche Stellen dienen. Ausgehend von den Schutzzielen sollten sanktionsbewehrte Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung gleichermaßen gelten. Dies betrifft etwa den Grundsatz der Zweckbindung, also das Prinzip, dass personenbezogene Daten ausschließlich für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Neu eingeführt werden sollte zudem ein grundsätzliches Verbot der Profilbildung. Die Vorgaben des allgemeinen Datenschutzrechts können – soweit erforderlich – in Bezug auf bestimmte Anwendungsgebiete weiter konkretisiert werden.

**Technikneutralen Ansatz schaffen**

Den aus der technologischen Entwicklung resultierenden Gefährdungen sollte durch technikneutrale Vorgaben begegnet werden, die auf konkrete Systeme und Anwendungsfelder durch Auslegung und Normierung konkretisiert werden können. Anhand festgelegter Schutzziele können so einfache, flexible und praxistaugliche gesetzliche Bedingungen geschaffen werden, die das Recht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch technischen und organisatorischen Datenschutz sichern.

**Betroffenenrechte stärken**

Dreh- und Angelpunkt zur Durchsetzung des Datenschutzes ist der aufmerksame und kritische Betroffene. Die Datenverarbeitung muss für die Betroffenen transparenter werden, etwa indem die Wahrnehmung des Auskunftsanspruchs erleichtert wird. Die Freiwilligkeit der Einwilligung in eine Datenverarbeitung muss gestärkt werden.

noch Anlage 6

Konferenz der Datenschutzbeauftragten des Bundes und der Länder
„Ein modernes Datenschutzrecht für das 21. Jahrhundert“

**Datenschutzrecht internetfähig machen**

Ein modernes Datenschutzrecht muss internetfähig sein. Grundsätzlich muss eine unbeobachtete Kommunikation und Nutzung des Internets gewährleistet werden. Auch sind besondere Schutzmechanismen zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen im Netz zu schaffen. Nationale Regelungen sollten durch internationale Vereinbarungen flankiert werden.

**Mehr Eigenkontrolle statt Zwang**

Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden. Dies kann etwa durch Einführung eines freiwilligen Auditverfahrens befördert werden. Daneben müssen die verantwortlichen Stellen dazu verpflichtet werden, durch interne Mechanismen die Einhaltung des Datenschutzes sicherzustellen, etwa durch verbindliche Datenschutzkonzepte.

**Stärkung der unabhängigen Datenschutzaufsicht**

Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten ist mit der EG-Datenschutzrichtlinie nicht vereinbar. Erforderlich sind auch Mitwirkungspflichten der kontrollierten Stellen bei Datenschutzkontrollen.

**Wirksamere Sanktionen**

Die immer noch vorhandenen Lücken im datenschutzrechtlichen Sanktionssystem müssen endlich geschlossen werden. Hierfür sollten für die Betroffenen einfach zu handhabende Haftungsansprüche, etwa ein pauschalierter Schadensersatzanspruch, eingeführt werden. Die Zuständigkeiten für die Verfolgung von Ordnungswidrigkeiten sollten bei den jeweiligen Datenschutzbehörden liegen. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit braucht insoweit wirksame Sanktionsbefugnisse.

**Gesetz einfacher und besser lesbar machen**

Das Datenschutzrecht ist durch wiederholte Änderungen und Ergänzungen selbst für Fachleute nur noch schwer verständlich und bedarf auch insoweit der Überarbeitung. Erforderlich sind etwa Änderungen in der Struktur und bei den Definitionen, die zusätzliche Spezialvorschriften entbehrlich machen.

4

# 2. Grundsätzliche Erwägungen

### *2.1 Zielbestimmungen und Grundstruktur des Gesetzes*

*Das Datenschutzrecht hat sich in seiner Grundstruktur in den letzten Jahrzehnten nicht verändert, obwohl sich die technischen Voraussetzungen der elektronischen Datenverarbeitung und der Umfang der dabei anfallenden personenbezogenen Daten und damit die Gefährdung des Persönlichkeitsrechts radikal gewandelt haben. Die Prämissen der Datenschutzgesetze entsprechen immer weniger den Bedingungen der heutigen technologischen und gesellschaftlichen Realität. Dies ist auch nicht verwunderlich, denn die wesentlichen Regelungskonzepte der Datenschutzgesetze stammen im Kern aus der Zeit der Großrechner, in der PCs und Internet noch unbekannt waren.*

*Eine Vielzahl von Spezialregelungen, die das Bundesdatenschutzgesetz (BDSG) ganz oder teilweise überlagern und verdrängen, haben das Recht für Anwenderinnen und Anwender wie Betroffene unübersichtlich und unverständlich gemacht. Obwohl das Bundesverfassungsgericht immer wieder die Bedeutung des Grundrechts auf informationelle Selbstbestimmung unterstrichen und dieses um das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ergänzt hat, tritt die eigentliche Zielsetzung des Datenschutzes immer mehr in den Hintergrund, nämlich der Einzelnen/dem Einzelnen als Ausfluss ihrer/seiner Menschenwürde die Verfügungsmacht über die ihre/seine Person kennzeichnenden und prägenden Informationen zu sichern und sie/ihn nicht zum bloßen Objekt der Informationsverarbeitung anderer werden zu lassen. Die allgegenwärtige Datenverarbeitung bedroht dabei nicht nur die Menschenwürde, sie beschneidet auch die Handlungs- und Verhaltensfreiheit der/des Einzelnen, etwa wenn diese/dieser in einem videoüberwachten Raum ihr/sein Verhalten der Tatsache dieser Dauerbeobachtung anpasst. Die informationelle Selbstbestimmung ist, wie das Bundesverfassungsgericht wiederholt festgestellt hat, eine unverzichtbare Grundbedingung der Demokratie.*

*Oberstes Ziel einer Modernisierung des Datenschutzrechts muss es deswegen sein, die Betroffenen als Grundrechtsträger wieder in den Mittelpunkt zu rücken und den wachsenden Gefährdungen ihrer Menschenwürde und Handlungs- und Verhaltensfreiheit durch die technische Entwicklung und die moderne Massendatenverarbeitung entgegenzutreten.*

Die Datenschutzreform sollte folgende wesentliche Elemente enthalten:

- Neue und konkrete Definition der Schutzziele des Datenschutzes als Grundlage und Maßstab aller datenschutzrechtlichen Regelungen und Maßnahmen:

5

noch Anlage 6



- In enger Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts müssen die Schutzziele des Datenschutzes neu und konkreter als bisher definiert und verbindlicher gestaltet werden. So sieht zwar bereits das geltende Datenschutzrecht beispielsweise eine Zweckbindung für die Verwendung personenbezogener Daten vor. Dieses auch vom Bundesverfassungsgericht als zentraler Grundsatz des Datenschutzrechts hervorgehobene Prinzip wird jedoch in der Praxis immer wieder in Frage gestellt und unterlaufen. Ziel muss es daher sein, dieses bei einer Modernisierung zu stärken und seine Bedeutung erneut zu betonen.
- Ausgangspunkt muss der Schutz der/des Einzelnen vor der Gefährdung (nicht nur konkreter Beeinträchtigung) ihrer/seiner Menschenwürde und Handlungs- und Verhaltensfreiheit durch das Sammeln und Verwenden ihrer/seiner personenbezogenen Daten sein, d.h. von Informationen über sie/ihn, ihr/sein Verhalten, ihren/seinen Aufenthalt und ihr/sein Denken. Dieser Schutz muss sich auch auf die von ihr/ihm genutzten elektronischen Hilfsmittel und Kommunikationsformen erstrecken, die ihre/seine Persönlichkeit abbilden können. Maßgeblich muss dabei die Gefährdung für das Persönlichkeitsrecht und die Eingriffsintensität sein: Je höher das Gefahrenpotenzial ist, desto wirkungsvollere Schutzmechanismen sind erforderlich.
- Der notwendige Schutz ist insbesondere gekennzeichnet durch
  - eine strikte Beschränkung der Datenverarbeitung und -nutzung auf das Erforderliche,
  - eine konsequentere Zweckbindung der einmal erhobenen personenbezogenen Daten (ausführlicher hierzu Abschnitt 2.2.2.),
  - die größtmögliche Selbstbestimmung der Betroffenen und
  - Transparenz der Datenverarbeitung (ausführlicher hierzu: Abschnitt 2.2.4.).
- Die Verwirklichung dieser Schutzziele soll durch folgende Maßnahmen unterstützt werden:
  - ein grundsätzliches Verbot der Profilbildung (ausführlicher hierzu: Abschnitt 2.2.3.) und
  - eine Verpflichtung zur konsequenten Löschung („geregeltes Vergessen“).

  Hierbei kann es grundsätzlich keinen Unterschied machen, ob die Gefährdung von einer öffentlichen oder von einer nicht-öffentlichen Stelle ausgeht.

6

- Stärkung des BDSG und der Datenschutzgesetze der Länder als allgemeingültige datenschutzrechtliche Grundregelungen:

  Neben dem allgemeinen Datenschutzrecht gibt es in Bund und Ländern eine Vielzahl von spezialgesetzlichen Regelungen, die ganz oder teilweise an die Stelle des allgemeinen Rechts treten, ohne dass dies oft eindeutig geklärt wäre. Nach § 1 Abs. 3 BDSG geht z.B. jede Rechtsvorschrift des Bundes, die auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden ist, dem BDSG vor. Diese weitgehende Subsidiarität des BDSG trägt maßgeblich zur Unübersichtlichkeit und Unverständlichkeit des Datenschutzrechts bei. Die allgemeinen Regeln des BDSG und der entsprechenden Landesgesetze müssen deswegen als allgemeine Grundregelungen verankert werden, denen spezialgesetzliche Bestimmungen nur noch ausnahmsweise vorgehen, wenn und soweit sie ausdrücklich und eindeutig davon abweichen.

- Gleiche Regeln für öffentliche und nicht-öffentliche Stellen:

  Für die Gefährdung des Persönlichkeitsrechts spielt es keine Rolle, ob diese von einer öffentlichen oder einer nicht-öffentlichen Stelle ausgeht. Die Grundrechte auf informationelle Selbstbestimmung und auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sind nicht nur Abwehrrechte gegenüber staatlichen Stellen. Die Rechtsordnung muss den Schutzgehalt dieser Grundrechte vielmehr auch im nicht-öffentlichen Bereich gewährleisten. Die Grundsätze des Datenschutzrechts gelten nach der Europäischen Datenschutzrichtlinie für den öffentlichen und nicht-öffentlichen Bereich gleichermaßen. Deswegen sollten soweit wie möglich gleiche Regeln für öffentliche und nicht-öffentliche Stellen gelten, insbesondere auch bei den Betroffenenrechten. Eine solche Vereinheitlichung würde zudem die Verständlichkeit des Rechts deutlich stärken.

- Integration des Datenschutzes in Produkte und Verfahren:

  Die bisherigen datenschutzrechtlichen Bestimmungen richten sich direkt nur an Anwenderinnen und Anwender und Betroffene, nicht aber an die Herstellerinnen und Hersteller sowie Entwicklerinnen und Entwickler von Produkten und Verfahren. Dadurch bleiben datenschutzrechtliche Belange bei der Entwicklung von Hard- und Software oft unberücksichtigt. Nachträglich aufgepfropfte Datenschutzmaßnahmen sind zudem vielfach ungenügend und unwirtschaftlich. Die technische Integration des Datenschutzes in Produkte und Verfahren, z.B. im Hinblick auf Datenvermeidung oder Datensparsamkeit sowie einfachen und wirkungsvollen Selbstdatenschutz der Nutzerinnen und Nutzer, würde dagegen spätere Datenschutzprobleme vermeiden helfen. Ähnlich wie bei der technischen Betriebssicherheit können Normen und Verfahren einen integrierten technischen Datenschutz fördern und gewährleisten. Dies ließe sich etwa dadurch erreichen, dass

noch Anlage 6



Aufsichtsbehörden Anordnungsbefugnisse erhalten, um „Schwarze Schafe“ zu kennzeichnen. Die Verleihung von Gütesiegeln und die Durchführung von Auditverfahren können wirkungsvolle, marktsteuernde Anreize für besseren Datenschutz setzen. Letztlich tragen auch effektive Betroffenenrechte dazu bei, dass sich datenschutzfreundliche Angebote durchsetzen.

- Verstärkte Grundrechtssicherung durch technische und organisatorische Verfahren:

  Der grundrechtliche Schutz der Privatsphäre erstreckt sich nicht nur auf rechtliche Anforderungen an die Zulässigkeit der Datenerhebung und Datenverarbeitung, er umfasst auch technische und organisatorische Maßnahmen. Dies ergibt sich nicht erst aus dem Urteil des Bundesverfassungsgerichts zur Onlinedurchsuchung und dem neuen Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme. Bereits der Grundsatz der Erforderlichkeit der Datenerhebung zieht technische und organisatorische Maßnahmen zu seiner Umsetzung nach sich.

- Datenschutz als Bildungsaufgabe festschreiben:

  Effektiver Datenschutz muss heute stärker denn je bei den Betroffenen ansetzen. Sie können nur dann verantwortungsbewusst handeln, wenn sie sich der Gefahren für ihr Persönlichkeitsrecht bewusst sind und wissen, wie ihr Handeln sich auf sie selbst und auf andere Menschen auswirkt. Außerdem brauchen sie Kenntnisse darüber, wie sie sich gegen Gefährdungen schützen können, die mit der Nutzung von Informationstechnik verbunden sind. Die Vermittlung des Datenschutzbewusstseins muss als gesamtgesellschaftliche Aufgabe verstanden werden. Entsprechender Regelungen bedarf es deswegen nicht nur in den Datenschutzgesetzen, sondern auch in den Lehrplänen der Schulen und bei sonstigen Bildungseinrichtungen.

- Besserer Schutz für Minderjährige:

  Bei der Wahrnehmung der Datenschutzrechte handelt es sich um Grundrechtsausübung, für die es keine starre Altersregel gibt. Da die datenschutzrechtliche Einwilligung und die Geltendmachung von Betroffenenrechten nicht immer rechtsgeschäftlichen Charakter haben, greift auch der Minderjährigenschutz des Bürgerlichen Gesetzbuchs nicht immer. Unter Umständen treten Elternrechte und eigenständige Rechtsausübung Minderjähriger in Konkurrenz, insbesondere bei der Nutzung des Internets. Gerade hier ist die Gefahr, dass die Gutgläubigkeit und Unerfahrenheit von Kindern und Jugendlichen ausgenutzt wird, besonders groß. Deswegen bedarf es auch im Interesse der Anwenderinnen und Anwender klarer Rege-

lungen, ab wann und unter welchen Voraussetzungen Minderjährige eigenständig einwilligen und ihre Betroffenenrechte wahrnehmen können.

Durch die vorgeschlagenen Maßnahmen werden die Betroffenen und die Gefährdung ihres Persönlichkeitsrechts durch die elektronische Datenverarbeitung mehr ins Zentrum des Datenschutzrechts gerückt. Dies muss Maßstab aller gesetzlichen Regelungen sein.

### *2.2 Grundsätze des Datenschutzes*

*Ausgehend von der Zielsetzung der Datenschutzgesetze und der Schutzziele für die Betroffenen sollten konkrete Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung und für alle Anwenderinnen und Anwender von Datenverarbeitung gleichermaßen gelten und sanktionsbewehrt sind.*

#### 2.2.1 Datenvermeidung und Datensparsamkeit, Erforderlichkeit

*Der Grundsatz, personenbezogene Daten nur insoweit zu verarbeiten, als sie für die Erfüllung einer konkreten Aufgabe erforderlich sind, ist bereits seit langem im Datenschutzrecht verankert. Er muss auch bei der Gestaltung der technischen Systeme berücksichtigt werden. Das Gebot der Datenvermeidung und Datensparsamkeit ist zwar auch im geltenden Datenschutzrecht schon enthalten (z.B. § 3 a BDSG), es hat als allgemeine Zielvorgabe bislang aber kaum Wirkung entfaltet. Vielfach werden aber Datenverarbeitungssysteme und -verfahren angeboten und eingesetzt, bei denen mehr Daten erhoben werden oder einfach nur als Nebenprodukt anfallen, als eigentlich nötig wären. Einmal entstandene Datenbestände stellen aber per se eine Gefährdung des Persönlichkeitsrechts dar, weil sie immer für irgendwelche Zwecke nutzbar sind und entsprechende Begehrlichkeiten wecken. Verstöße gegen den Grundsatz der Datenvermeidung und Datensparsamkeit haben bislang keinerlei Konsequenzen zur Folge.*

Zur Stärkung des Grundsatzes der Datenvermeidung und Datensparsamkeit werden folgende Regelungen vorgeschlagen:

- Konkretisierung des verfassungsrechtlichen Grundsatzes der Datenvermeidung und Datensparsamkeit.
- Anspruch der Betroffenen, für den konkreten Zweck nicht erforderliche Daten auch nicht zu erheben und zu verarbeiten, und Anspruch darauf, die von der verantwortlichen Stelle eingesetzten Systeme und Verfahren entsprechend auszurichten.

9

noch Anlage 6



- Möglichkeit der Sanktionierung bei Nichtbeachtung dieses Grundsatzes.
- Schaffung eines datenschutzfreundlichen Identitätsmanagements: Das Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren.
- Verpflichtung, generell pseudonyme und anonyme Nutzungsmöglichkeiten anzubieten.
- Privacy by Design: Bevor ein neues System zur Erfassung personenbezogener Daten eingeführt wird, sollen die verantwortlichen Stellen sicherstellen, dass Datenschutzlösungen von Anfang an fest eingebaut werden und nicht erst in einem späteren Stadium hinzugefügt werden müssen.

Durch eine entsprechende Regelung könnte der Grundsatz der Datenvermeidung und Datensparsamkeit zu einer verbindlichen Norm werden, auf die sich Betroffene berufen können und deren Einhaltung von der Datenschutzaufsicht kontrolliert werden kann.

### 2.2.2 Grundsatz der Zweckbindung

*Der Grundsatz der Zweckbindung, also das Prinzip, dass personenbezogene Daten ausschließlich für den Zweck verwendet werden dürfen, für den sie erhoben worden sind, und sofort zu löschen sind, wenn sie für diesen Zweck nicht mehr erforderlich sind, hat herausragende Bedeutung für die Gewährleistung des Persönlichkeitsrechts. In der datenschutzrechtlichen Praxis kann die Zweckbindung ihre ursprüngliche Schutzfunktion aber immer weniger ausfüllen, weil es häufig an einer klaren Zweckbestimmung bei der ursprünglichen Erhebung der Daten fehlt, zahlreiche Vorschriften unter sehr allgemein formulierten Voraussetzungen Zweckänderungen zulassen und eine zweckfremde Verwendung von Daten vielfach keine Konsequenzen nach sich zieht. Eine konsequente Zweckbindung personenbezogener Daten korrespondiert zudem mit dem verfassungsrechtlichen Gebot zur informationellen Gewaltenteilung.*

Die folgenden Regelungen sollen die Zweckbindung stärken:

- Eine eigenständige Norm zur Zweckbindung unter den Datenschutzgrundsätzen, die
  - vor jeder Erhebung personenbezogener Daten eine konkrete Zweckbestimmung vorschreibt (Verbot der Vorratsdatenspeicherung),

- eine strikte Zweckbindung von als „Beifang“ anfallenden Daten ohne gezielten Personenbezug enthält, sofern die vorrangige Löschung oder Sperrung dieser Daten nicht möglich ist,
- eine strikte Zweckbindung für die Verwendung von Daten zu Zwecken der Datenschutzkontrolle, zur Datensicherheit oder zur Sicherstellung des ordnungsgemäßen Betriebs von Datenverarbeitungssystemen vorsieht.

- Zweckändernde Verwendungen von personenbezogenen Daten dürfen nur in klar definierten Ausnahmefällen zugelassen werden; gesetzlich vorgesehene Zweckbestimmungen dürfen nicht durch die Einwilligung der Betroffenen umgangen werden.
- Verstöße gegen die Zweckbindung müssen bußgeldbewehrt sein.
- Regelmäßiges Verwertungsverbot für Daten, die durch eine rechtswidrige Änderung des ursprünglichen Erhebungszwecks erlangt worden sind.

Eine verbesserte Zweckbindung stärkt die Selbstbestimmung der Betroffenen über den Umgang mit ihren persönlichen Daten und begegnet der zunehmenden Vernetzung unterschiedlicher Datenbestände, die auch vom Bundesverfassungsgericht als große Gefahr für das Persönlichkeitsrecht gesehen wird.

### 2.2.3 Verbot der Profilbildung

*Die Zusammenführung und Verknüpfung personenbezogener Daten zu Profilen stellt eine besondere Gefahr für das Persönlichkeitsrecht dar. Auf diese Weise können die Persönlichkeit eines Menschen, sein Verhalten, seine Interessen und Gewohnheiten verfügbar und vorhersehbar gemacht werden, was u.a. eine gezielte Manipulation erlaubt, ohne dass sich die Betroffenen dessen überhaupt bewusst sind. Derartige Profile gibt es bereits in vielen Bereichen, etwa als Konsumentenprofil, Bewegungsprofil, Nutzerprofil im Internet etc. Der rasante technologische Fortschritt in vielen Bereichen lässt Unmengen an personenbezogenen Daten anfallen, oft nur als Nebenprodukt, deren Verknüpfung immer ausgefeiltere Profile möglich macht.*

Zum Schutz der Betroffenen halten die Datenschutzbeauftragten des Bundes und der Länder deswegen folgende Maßnahmen für erforderlich:

- Eine gesetzliche Definition der Profilbildung.
- Die Bildung von Profilen sollte nur zulässig sein bei entsprechender konkreter gesetzlicher Grundlage, die dem besonderen Gefährdungspotential

noch Anlage 6



von Profilbildung Rechnung trägt, oder bei einer Einwilligung der/des Betroffenen.

- Eine wirksame Einwilligung setzt eine umfassende Information über Umfang und Herkunft der verwandten Daten, Zweck und Verwendung des Profils, verantwortliche Stelle und vorgesehene Löschungsfrist voraus.
- Die Einwilligung muss freiwillig und jederzeit widerrufbar sein. Der Widerruf muss die sofortige Löschung des Profils zur Folge haben, auch bei den Stellen, an die es übermittelt worden ist.

Nur durch eine strikte Reglementierung der Profilbildung kann in diesem besonders sensiblen Bereich die informationelle Selbstbestimmung gewährleistet werden.

### 2.2.4 Wahrung der Transparenz – Offene Datenverarbeitung

*Die moderne Datenverarbeitung ermöglicht in erheblichem Umfang eine für die Betroffenen nicht offensichtliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Das Datenschutzrecht enthält eine Reihe von Vorschriften für eine transparente Datenerhebung (und Weiterverarbeitung), die in der Regel an bestimmte Technologien anknüpfen (Videoüberwachung, Chipkarten usw.). Es fehlt aber an einem übergreifenden technikunabhängigen Konzept. Auf der anderen Seite entstehen in großem Umfang ungezielt – quasi nebenher – bei der Inanspruchnahme informationstechnischer Systeme personenbeziehbare Daten (z. B. Protokoll- oder Verkehrsdaten), bei denen die unmittelbare Herstellung des Personenbezugs nicht intendiert, aber möglich ist. Diese Daten können sensitiv sein, da sie umfassende Auskünfte über die Verhaltensweise der/des Einzelnen geben können. Hierfür gibt es im geltenden Datenschutzrecht keine adäquaten Lösungen.*

*Ein spezifisches Problem intransparenter Datenerhebung (sowie Verarbeitung und Nutzung) ist die Ortung, d. h. die Feststellung des geografischen Standortes oder der räumlichen Bewegung von Personen oder Gegenständen, die Personen zugeordnet werden können. Hierfür bietet bisher nur das Telekommunikationsrecht eine bereichsspezifische Lösung an.*

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schlägt vor, zur Wahrung der transparenten Datenerhebung, -verarbeitung und -nutzung eine einheitliche, technikunabhängige Norm zu schaffen. Folgende Eckpunkte müssen dabei berücksichtigt werden:

- Mikrotechnologie und Digitalisierung ermöglichen in zunehmendem Maße die vom Betroffenen unbemerkte Datenerhebung. Daten können ungezielt,

fast zufällig und als „Beifang“ der eigentlichen Prozesse erhoben werden. Hier ist für die Betroffenen größtmögliche Transparenz herzustellen. Dies bedeutet, dass die Erhebung personenbezogener Daten für die Betroffenen transparent sein muss und umgekehrt eine von den Betroffenen unbemerkbare Datenerhebung grundsätzlich verboten wird.

- Die Transparenz der Erhebung personenbezogener Daten zeichnet sich dadurch aus, dass die Betroffenen angemessen über die beabsichtigte Erhebung (und weitere Verwendung) der Daten zu informieren sind. Dafür sollten die Transparenzvorschriften einheitlich zusammengefasst werden:
  - Die Datenerhebung muss für die Betroffenen erkennbar sein. Die Funktionsweise und Art der zu erhebenden und verwendenden Daten müssen in verständlicher Form erkennbar gemacht werden.
  - Die Identität der verantwortlichen Stelle ist durch geeignete Maßnahmen erkennbar zu machen.
  - Die Betroffenen müssen in geeigneter Weise darüber informiert werden, wie sie ihre Rechte geltend machen können.
  - Die verantwortlichen Stellen müssen eine detaillierte Datenschutzerklärung in geeigneter Weise auf aktuellem Stand zugänglich halten.
- In diesem Sinne von den Betroffenen unbemerkt, dürfen Daten erhoben werden, wenn sie ausschließlich zu dem Zweck verarbeitet werden, die Nutzung automatisierter Verfahren und die automatische Kommunikation zwischen Datenverarbeitungsanlagen technisch zu ermöglichen. Dies muss auch für solche Daten gelten, die grundsätzlich geeignet sind, nachträglich auf einzelne Personen bezogen zu werden. Für diese Daten gilt:
  - Das Gebot der Datenvermeidung sollte gestärkt werden.
  - Die Daten sind unmittelbar nach Erfüllung ihres Zwecks zu löschen, ohne dass es auf eine entsprechende Aktivität der Betroffenen ankommt.
  - Die Daten dürfen (nach dem Vorbild von §§ 14 Abs. 4, 31 BDSG) nur für den Zweck der technischen Ermöglichung der Kommunikation verarbeitet und genutzt werden, was durch geeignete technische und organisatorische Maßnahmen abzusichern ist.
  - Die Daten sollten einem Verbot der weiteren Verwendung unterliegen, um Profilbildung und Verknüpfung zu verhindern.
  - Die notwendige Transparenz ist auch hier durch Datenschutzerklärung herzustellen.
  - Zur Unterstützung der o. g. Prinzipien ist der Einsatz datenschutzfreundlicher Technologien vorzuschreiben.
  - Verstöße sind mit wirksamen Sanktionen zu ahnden.

13

- Zu prüfen ist, ob und inwieweit das Auskunftsrecht weiterhin auch für diese nur flüchtig gespeicherten Daten gelten soll.

- Die Voraussetzungen, unter denen eine Erhebung gestattet wird, sind technikneutral zu regeln. Nicht auf die Regulierung der einzelnen Techniken, sondern auf die Festlegung von Schutzzielen ist Wert zu legen (siehe Kapitel 3).
- Es ist eine allgemeine und technikunabhängige Regelung zur Verarbeitung von personenbezogenen Lokalisierungsdaten zu schaffen, die sich an den jeweiligen Risiken orientiert:
  - Die Tatsache der konkreten Ortung ist den Betroffenen in verständlicher Form anzuzeigen, etwa durch ein akustisches Signal, sobald die/der Betroffene geortet wurde.
  - Beim Einsatz von Tracking-Systemen, also jede Form der Ortung durch Dritte, die Betroffene nicht beeinflussen können, ist die Einwilligung (nach dem Vorbild von § 98 TKG) vorzusehen.
- Selbst bei einer heimlichen, aber nach bereichsspezifischem Recht erlaubten Datenerhebung sind geeignete und effektive Benachrichtigungspflichten vorzusehen.

Es sollte eine allgemeine technikunabhängige Vorschrift zur transparenten Datenerhebung, -verarbeitung und -nutzung geschaffen werden.

Die gezielte heimliche Datenerhebung wird nur in Ausnahmefällen z. B. zur Strafverfolgung erlaubt, im Übrigen grundsätzlich untersagt. Das Verbot wird durch Verwertungsverbote und Sanktionen abgesichert.

### *2.3 Beteiligung mehrerer Stellen an der Datenverarbeitung/Cloud Computing*

*Das BDSG kennt – ebenso wie eine Reihe von Landesdatenschutzgesetzen – keine ausdrückliche Regelung für eine gemeinsame Verarbeitung personenbezogener Daten durch mehrere Stellen. Anders als die Europäische Datenschutzrichtlinie kennt das BDSG beim Begriff der verantwortlichen Stelle nicht die Möglichkeit einer gemeinsamen Verantwortlichkeit mehrerer Stellen („joint controllership“). Eine wachsende Bedeutung kommt in der Praxis zentralen IT-Verfahren zu, an denen verschiedene Stellen von Bund und Ländern, mehrere Länder oder gar nicht-öffentliche Stellen beteiligt sind.*

*Es ist außerordentlich schwierig, solche Verfahren gesetzeskonform zu betreiben, weil die klassischen Instrumente Auftragsdatenverarbeitung oder Übermittlung nicht passen und zudem völlig unterschiedliche und z. T. einander widersprechende datenschutzrechtliche Normen des Bundes und der Länder*

*beachtet werden müssten. Außerdem sind u. U. zahlreiche Kontrollbehörden für die datenschutzrechtliche Kontrolle nebeneinander zuständig.*

*Weitere Fragen wirft auch die verteilte und häufig grenzüberschreitende Datenverarbeitung auf, wie es z. B. beim Cloud Computing oder beim Binnenmarktinformationssystem IMI der Fall ist. Solche Konstellationen sind mit dem Datenschutzrecht nicht befriedigend in Einklang zu bringen. Das Instrument der Auftragsdatenverarbeitung lässt sich in der Praxis nicht umsetzen. Legt man die Funktionsübertragung (mit Übermittlung von Daten zwischen den beteiligten Stellen) zugrunde, ist die Verteilung der Verantwortlichkeiten nicht befriedigend zu regeln.*

Aus diesen Gründen sollte das Konzept der Zuweisung von Verantwortlichkeiten neu gefasst werden:

- Der Begriff der verantwortlichen Stelle ist an dem Vorbild von Art. 2 lit. d) der EG-Datenschutzrichtlinie zu orientieren.
- Die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung ist bei der Beteiligung mehrerer Stellen durch entsprechende Vorschriften von den tatsächlichen Einflussmöglichkeiten und der Interessenlage der Betroffenen abhängig zu machen (Prinzip der Accountability). Die datenschutzrechtliche Verantwortlichkeit kann demnach z. B. auch nach einer Übermittlung fortbestehen, wenn die wirtschaftlichen bzw. tatsächlichen Einwirkungsmöglichkeiten auf die Empfänger dafür vorhanden sind.

Für gemeinsame Verfahren müssten folgende Anforderungen berücksichtigt werden:

- Festlegung materieller und formeller Anforderungen an die Zulässigkeit gemeinsamer Verfahren (Abwägung mit den schutzwürdigen Belangen Betroffener; bei Verfahren mit erheblicher Bedeutung ggf. gesonderte Rechtsgrundlage).
- Integration der Vorschriften zu den Abrufverfahren (§ 10 BDSG) als eine Form des gemeinsamen Verfahrens.
- Einführung spezifischer technischer und organisatorischer Sicherungen (z. B. zwingende Vorabkontrolle).
- Verpflichtung, die Verantwortlichkeiten für die Umsetzung der fachlichen und technischen Vorgaben eindeutig festzulegen.
- Verpflichtung, die Verantwortlichkeiten für die Rechtmäßigkeit der Datenverarbeitung zu dokumentieren.

noch Anlage 6



- Verpflichtung, sowohl das anwendbare Datenschutzrecht als auch die zuständigen Datenschutzkontrollbehörden zu regeln.
- Sicherstellung, dass die Betroffenen gegenüber jeder beteiligten Stelle ihre Rechte geltend machen können.

Die Neufassung des Begriffs der verantwortlichen Stelle sowie die Einführung des Prinzips der nachhaltigen Verantwortlichkeit („Accountability“) ermöglichen vor allem bei der Beteiligung mehrerer Stellen an der Datenverarbeitung eine interessengerechte Verteilung der Verantwortlichkeit. Jede Stelle ist verantwortlich, wenn und soweit sie in tatsächlicher Hinsicht über Mittel und Zwecke der Datenverarbeitung verantwortlich bestimmen kann. Die Betroffenen können ihre Rechte gegenüber jeder verantwortlichen Stelle geltend machen.

### *2.4 Datenverarbeitung im Auftrag*

*Bei der Einbeziehung Dritter im Rahmen der Auftragsdatenverarbeitung hat der Gesetzgeber durch die letzten Änderungen des § 11 BDSG Präzisierungen und Klarstellungen vorgenommen, deren Auswirkungen zunächst abzuwarten sein werden. Ungelöst ist allerdings nach wie vor die Frage der zulässigen Auftragsdatenverarbeitung, wenn die Daten bei der Auftraggeberin/beim Auftraggeber durch Berufsgeheimnisse i. S. v. § 203 StGB geschützt sind. Da die Weitergabe der Daten an die Auftragnehmerin/den Auftragnehmer zwar keine datenschutzrechtliche Übermittlung, wohl aber eine Offenbarung des Geheimnisses darstellt, gibt es hierfür keine Rechtsgrundlage. So kann die Inanspruchnahme von IT-Dienstleistungen durch Ärztinnen und Ärzte, Rechtsanwältinnen und Rechtsanwälte und Steuerberaterinnen und Steuerberater, aber auch durch Versicherungen in vielen Fällen nur auf die Einwilligung der Betroffenen gestützt werden. Gleiches gilt z.B. für die externe Archivierung von Patientenakten in Krankenhäusern, sofern das Landeskrankenhausrecht hier keine ausdrückliche Befugnis enthält.*

*Ein weiteres Problem ist die Auftragsdatenverarbeitung bei besonders sensitiven Daten (§ 3 Abs. 9 BDSG), wenn die Auftragnehmerin/der Auftragnehmer ihren/seinen Sitz in einem Drittland außerhalb der EU hat. Da hierfür die Übermittlungsvorschriften zu beachten sind (vgl. § 3 Abs. 8 Satz 3 BDSG), ist eine Auftragsdatenverarbeitung unter diesen Umständen – anders als in anderen Mitgliedstaaten der EU – kaum möglich.*

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält folgende Schritte für notwendig:

- Schaffung einer eng begrenzten Offenbarungsbefugnis z.B. in § 11 BDSG und den vergleichbaren Vorschriften der Landesdatenschutzgesetze, um eine Strafbarkeit der Berufsgeheimnisträgerinnen und -träger auszuschließen.
- Einbeziehung der Auftragnehmerinnen und Auftragnehmer in die strafrechtliche Sanktionierung bei Verstößen gegen das Berufsgeheimnis (etwa durch Gleichstellung mit den Berufsgehilfen in § 203 Abs. 3 Satz 2 StGB).
- Schaffung der notwendigen strafprozessualen Begleitmaßnahmen (Zeugnisverweigerungsrecht, Beschlagnahmeschutz).

Für die Auftragsdatenverarbeitung in Drittländern ist eine spezifische Norm zu schaffen, die diese nicht von den Übermittlungsvoraussetzungen, sondern vom angemessenen Datenschutzniveau im Drittland abhängig macht.

Die Schaffung einer Offenbarungsbefugnis für eine Auftragsdatenverarbeitung durch Berufsgeheimnisträger würde es auch diesen Berufsgruppen in begrenztem Umfang ermöglichen, insbesondere IT-Dienstleistungen durch Dritte durchführen zu lassen.

Die Möglichkeit, grundsätzlich auch sensitive Daten in Drittstaaten außerhalb der EU im Auftrag verarbeiten zu lassen, würde Wettbewerbsnachteile deutscher Unternehmen gegenüber anderen europäischen Unternehmen beseitigen und insofern Chancengleichheit herstellen.

noch Anlage 6

Konferenz der Datenschutzbeauftragten des Bundes und der Länder
„Ein modernes Datenschutzrecht für das 21. Jahrhundert“

## 3. Technischer und organisatorischer Datenschutz

*Das Recht auf informationelle Selbstbestimmung kann nur gewährleistet werden, wenn es durch besondere Vorkehrungen für die technische Durchführung und Organisation der Erhebung, Verarbeitung und Nutzung personenbezogener Daten gesichert wird. Angesichts der weit fortgeschrittenen Digitalisierung der automatisierten Datenverarbeitung und ihrer Allgegenwart, angesichts der Verkettbarkeit personenbezogener Daten kommt technischen und organisatorischen Schutzvorkehrungen eine immer größere Bedeutung zu. Die besten rechtlichen Verarbeitungsbeschränkungen sind praktisch wertlos, wenn ihre technische und organisatorische Absicherung fehlt oder mangelhaft ist.*

*Die Konzeption des BDSG und vieler Landesdatenschutzgesetze wird diesen Anforderungen indes nicht mehr gerecht. Die in der Anlage zu § 9 BDSG aufgeführten einzelnen Maßnahmen zur Gewährleistung des technischen und organisatorischen Datenschutzes stammen noch aus der Zeit der Großrechnertechnologie und lassen sich nur noch mit Mühe auf die heutige Welt vernetzter und ubiquitärer Systeme übertragen. Es ist zu erwarten, dass sie für die weitere Entwicklung der IuK-Technologien noch weniger geeignet sein werden.*

*Im geltenden Recht finden sich nur punktuelle Lösungsansätze hinsichtlich der konzeptionellen Absicherung vor Datenschutzrisiken beim Einsatz automatisierter Verfahren. Dies betrifft auch Verfahren, bei denen eine Verarbeitung personenbezogener Daten nicht von vornherein intendiert, aber (ggf. zu einem späteren Zeitpunkt) möglich ist.*

Die Konferenz der Datenschutzbeauftragten schlägt deshalb eine grundsätzliche Reform der Regeln zum technischen und organisatorischen Datenschutz vor, die folgende Aspekte berücksichtigen müsste:

- Die bisher in der Anlage zu § 9 BDSG beschriebenen Maßnahmen zur Gewährleistung des technischen und organisatorischen Datenschutzes („10 Gebote“) sind durch die Definition elementarer Schutzziele zu ersetzen. Diese sollten folgende Bedingungen erfüllen:
  - Die Schutzziele sollten einfach, verständlich und praxistauglich sein.
  - Die Schutzziele sind an den Vorgaben des Datenschutzes zu messen, müssen längere Zeit Bestand haben und dürfen sich trotz aller Überschneidungen nicht allein an den Vorgaben der IT-Sicherheit orientieren.
  - Aus den Schutzzielen sollten sich die konkret in der Praxis zu treffenden Maßnahmen ableiten lassen. Die Maßnahmen müssen in einfa-

chen, flexiblen und praxistauglichen Verfahren – durch Software unterstützt – umgesetzt werden können. Sie können die Basis für die Kriterien eines Datenschutzaudits bilden.

- Die Schutzziele müssen technologieunabhängig definiert werden.
- Die Schutzziele sind nachhaltig. Lediglich die Maßnahmen sind dem Stand der Technik anzupassen.
- Die Schutzziele sind so zu fassen, dass grundsätzliche rechtliche Anforderungen (z. B. Datenvermeidung/Datensparsamkeit, Zweckbindung oder Betroffenenrechte wie Berichtigung oder Löschung) technisch umgesetzt werden können.

- Entsprechend den genannten Anforderungen sind folgende Schutzziele aufzunehmen:
  - Verfügbarkeit
  - Vertraulichkeit
  - Integrität
  - Transparenz
  - Nichtverkettbarkeit (als technische Sicherung der Zweckbindung)
  - Intervenierbarkeit (als technische Gestaltung von Verfahren zur Ausübung der Betroffenenrechte)
- Die Umsetzung der Schutzziele durch technische und organisatorische Maßnahmen ist konzeptionell abzusichern:
  - Vor der Freigabe von Verfahren sind grundsätzlich die Risiken für das Recht auf informationelle Selbstbestimmung zu analysieren und die zur Beherrschung der Risiken zu treffenden Maßnahmen in einem Sicherheitskonzept zu beschreiben; das Sicherheitskonzept ersetzt nicht die Vorabkontrolle, sondern ist deren Bestandteil. Es kann zudem wichtige Grundlage eines Datenschutzmanagements sein.
  - Risikoanalyse und Sicherheitskonzept sind nach dem Stand der Technik regelmäßig fortzuschreiben.
- Die Umsetzung der Schutzziele muss konzeptionell zu einem möglichst frühen Zeitpunkt ansetzen:

  Technische und organisatorische Maßnahmen sind im Sinne eines vorgelagerten Systemdatenschutzes schon dann zu treffen, wenn in einem Verfahren die Möglichkeit besteht, dass personenbezogene Daten verarbeitet werden oder dass dies zu einem späteren Zeitpunkt intendiert ist.
- Angesichts der hohen Komplexität informationstechnischer Systeme ist eine gesetzliche Verpflichtung der verantwortlichen Stellen zu schaffen, den Betroffenen Methoden und Mittel des Selbstdatenschutzes zur Verfü-

noch Anlage 6



gung zu stellen; der Staat hat die Verpflichtung, die informationelle Selbstverantwortung und das Prinzip des Selbstdatenschutzes zu fördern.

- Die Regelungsvorschläge gelten – wie bisher – gleichermaßen für den nicht-öffentlichen und wie den öffentlichen Bereich.

Mit den o. g. Regelungsvorschlägen werden einfache, flexible, und praxistaugliche gesetzliche Bedingungen geschaffen, das Recht auf informationelle Selbstbestimmung durch technischen und organisatorischen Datenschutz zu sichern. Durch die technologieunabhängige Definition der Schutzziele ist die Nachhaltigkeit gewährleistet, sodass keine fortlaufenden Anpassungen notwendig werden und das Recht nicht permanent der Technik hinterherhinkt.

Defizite bei der Umsetzung der technischen und organisatorischen Maßnahmen können durch dokumentierte Risikoanalysen und Sicherheitskonzepte abgebaut werden.

Mit den Vorschlägen kann der Einsatz datenschutzfreundlicher Technologien – auch zur Stärkung der Eigenverantwortung und des Selbstdatenschutzes der Betroffenen – gefordert und gefördert werden.

20

noch Anlage 6



# 4. Betroffenenrechte

## *4.1 Mehr Transparenz in der Datenverarbeitung*

*Dreh- und Angelpunkt zur Durchsetzung des Datenschutzes ist der aufmerksame und kritische Betroffene. Doch nur wenn sie oder er ihre/seine Rechte einfach und effektiv geltend machen kann, wird sie/er diese auch nutzen. Das derzeitige Recht kennt zwar bereits eine Reihe von Rechten auf Auskunft, Berichtigung und Löschung. Es kommt aber darauf an, dass die Betroffenen diese Rechte unkompliziert geltend machen können. Hierzu kann auch eine regelmäßige Benachrichtigung über die gespeicherten personenbezogenen Daten (Datenbrief) einen Beitrag leisten.*

Die Konferenz der Datenschutzbeauftragten fordert, das bestehende Datenschutzrecht um folgende Punkte zu ergänzen:

- Erweiterung der Informationspflichten (etwa nach § 4 BDSG):
  - Die Verantwortlichkeit für die Datenverarbeitung muss gegenüber den Betroffenen klar und eindeutig offengelegt werden.
  - Die Kerninformationen müssen an prominenter Stelle platziert werden, statt mehrseitige, kleingedruckte Einwilligungserklärungen zum Datenschutz zu verwenden.
- Umgekehrt bedeutet dies als Pflicht für die verantwortliche Stelle: Dokumentation der Herkunft und der Empfänger von Daten sowie Protokollierung von Datenbankzugriffen.
- Vereinfachte Auskunftsrechte der Betroffenen:
  - Leichter Zugang zu Informationen über gespeicherte personenbezogene Daten („Mein XYZ“); Bereitstellung technischer Mittel zur Erleichterung der Wahrnehmung von (Datenschutz-)Rechten.
  - Generelle Einführung eines Rechts auf elektronische Auskunftserteilung/Einsichtnahme für die Betroffenen.
  - Auskunftsrecht der Betroffenen auch hinsichtlich der Zusammenführung ihrer Daten mit anderen Daten.
  - Erstreckung des Auskunftsrechts auf die Nutzung, soweit sie vom Zweck der Datenerhebung abweicht.
- Aufklärung über Risiken und Information über Datenpannen auch im öffentlichen Bereich.

noch Anlage 6



- Auskunfteien und Detekteien sollten die Auskunft nicht mehr unter Berufung auf
überwiegende Geschäftsgeheimnisse verweigern dürfen.

### *4.2 Echte Einwilligung statt faktischem Zwang*

*Die allgegenwärtige Datenverarbeitung ist aus der Informationsgesellschaft nicht mehr wegzudenken. Die Einwilligung der Betroffenen ist im Allgemeinen in der Privatwirtschaft eine wichtige Ermächtigungsgrundlage für eine Datenverarbeitung. Um wirksam zu sein, muss sie insbesondere freiwillig und informiert erteilt werden. Angesichts der immer komplexer werdenden Welt der allgegenwärtigen Datenverarbeitung ist dies fast schon Illusion. Es kommt darauf an, den Betroffenen die immer umfassenderen Datenverarbeitungen nicht zu verheimlichen, sondern einfach und verständlich die wichtigsten Konsequenzen zu erläutern, damit die Betroffenen sich bei Interesse vertiefter informieren können, im Übrigen aber ein Verständnis für die Welt der Informationsgesellschaft entwickeln und sich selbstbestimmt darin entfalten können.*

Die Konferenz der Datenschutzbeauftragten fordert, das bestehende Datenschutzrecht um folgende Punkte zu ergänzen:

- Die Einwilligung muss durch aktives Tun (ankreuzen, Haken setzen etc.) erteilt werden, eine formularmäßige Einwilligung, etwa durch Unterschrift unter allgemeine Geschäftsbedingungen oder umfangreiche Datenschutzerklärungen, genügt nicht.
- Die Geltungsdauer einer Einwilligung wird zeitlich begrenzt, da Betroffene nach einer gewissen Zeit die Konsequenzen nicht mehr einschätzen können oder im Bereich der Werbung die Daten häufig „wandern“ und die Betroffenen unter Umständen Mühe haben, eine einmal erteilte Einwilligung gegenüber allen „Nutznießern“ zu widerrufen.
- Anspruch auf Nachweis der Einwilligung, um den Betroffenen eine wirksame Durchsetzung ihrer Ansprüche zu ermöglichen.
- Der Widerruf sollte nur bei der Stelle eingelegt werden müssen, die die Daten erstmalig weitergegeben hat. Diese hat den Widerspruch dann an die Empfänger der Daten weiterzugeben.
- Das Koppelungsverbot im Bereich der Werbung sollte strenger formuliert werden. Der Abschluss eines Vertrages darf bereits heute nicht davon ab-

hängig gemacht werden, dass die oder der Betroffene in die Weitergabe ihrer oder seiner persönlichen Daten an Dritte zu Werbezwecken einwilligt, es sei denn, die Datenweitergabe ist gerade Gegenstand des Vertrages. Dieses Verbot sollte ausgeweitet und nicht auf marktbeherrschende Unternehmen beschränkt werden. Soweit das Koppelungsverbot von dem Merkmal der „Marktbeherrschung“ abhängig ist, besteht die Gefahr, dass nicht marktbeherrschende Unternehmen dies als Ermutigung zur Koppelung verstehen. Darüber hinaus sollte das Koppelungsverbot über den Bereich der Werbung hinaus ausgedehnt werden.

- Der Widerruf der Einwilligung darf nicht durch einen Medienbruch erschwert werden („Wieso darf zwar die Einwilligung elektronisch erklärt werden, nicht aber der Widerspruch zur Werbenutzung?“).

Eine derart reformierte Einwilligungserklärung versetzt die Betroffenen wieder in die Lage, ihre Daten selbst zu kontrollieren und sich verständig in der Informationsgesellschaft zu bewegen.

noch Anlage 6

Konferenz der Datenschutzbeauftragten des Bundes und der Länder
„Ein modernes Datenschutzrecht für das 21. Jahrhundert“

## 5. Datenschutz im Internetzeitalter

*Das Internet ist weder rechtsfreier Raum noch harmlose Spielwiese. Es gehört zur Lebenswirklichkeit in der Informationsgesellschaft. Immer stärker wird der Druck, Teil des globalen Netzes zu sein – ob nun freiwillig in sozialen Netzwerken oder unfreiwillig als Objekt der Bewertung, Kritik, aber auch Verleumdung. Die Konferenz der Datenschutzbeauftragten fordert daher, die Stärkung des Datenschutzes im Internet als gesellschaftliche Aufgabe zu verstehen, die von allen relevanten gesellschaftlichen und staatlichen Akteurinnen und Akteuren getragen werden muss.*

*Ein modernes Datenschutzrecht muss internetfähig sein. Die globale Struktur des Internets und neue Dienste, wie z.B. Street View und Soziale Netzwerke, setzen nationalen Regelungsansätzen und -strategien jedoch enge Grenzen. Die Globalisierung ist allerdings keine Entschuldigung für nationale Passivität. Es ist daher ein mehrdimensionaler Ansatz zur Stärkung des Datenschutzes zu verfolgen: Nationale Regelungen sollten möglichst durch internationale Vereinbarungen flankiert werden, so dass ein weitgehend deckungsgleiches inhaltliches Grundniveau des Internet-Datenschutzes entsteht, dem sich Anbieter von Diensten nicht ohne weiteres durch Flucht in das Ausland entziehen können. Gleichzeitig müssen vollzugsfähige Strukturen geschaffen werden, die es ermöglichen, dass gemeinsam anerkannte Standards auch international durchgesetzt werden können.*

Bei der Fortentwicklung des Internetrechts ist ein rechtlicher Rahmen zu schaffen, der die grundsätzlich unbeobachtete Kommunikation und Nutzung des Internets gewährleistet. Zudem hält die Konferenz die Entwicklung von besonderen Schutzmechanismen zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen im Netz für erforderlich. Angesichts der weltweiten Vernetzung und dauerhaften Verfügbarkeit von Inhalten im Netz besteht im Internet eine besondere Gefährdungslage, der nur durch internetspezifische Instrumente begegnet werden kann. Im Einzelnen schlägt die Konferenz vor allem vor, das bestehende Datenschutzrecht um folgende Punkte zu ergänzen:

- Einführung eines Mediennutzungsgeheimnisses, das die grundsätzlich unbeobachtete Inanspruchnahme elektronischer Dienste garantiert.
- Stärkung der Möglichkeit zur anonymen und pseudonymen Nutzung und Bezahlung von Online-Angeboten.
- Verbesserte Informationspflichten für Anbieter:
  - Wichtigste Datenschutzinformation an prominenter Stelle des Webauftritts: Ort der Datenspeicherung, zuständige Datenschutzbehörde

- Verpflichtung, die Nutzerinnen und Nutzer über alle Änderungen der Datenschutz- und Geschäftsbedingungen vorab in Kenntnis zu setzen und diese zu dokumentieren.

- „Privacy first“ oder „privacy by default“, d.h. Grundeinstellung von Internetdiensten müssen ein Optimum an Datenschutz bieten, Abweichungen hiervon sind von den Nutzenden im Sinne einer Opt-In-Lösung selbstverantwortlich zu wählen.
- Verpflichtung der Anbieter, den Betroffenen neben der Möglichkeit zur elektronischen Erteilung der Einwilligung auch einen elektronischen Zugriff auf ihre Daten und die elektronische Ausübung von Widerspruchs-, Berichtigungs- und Kündigungsrechten ohne diskriminierenden Medienbruch zu ermöglichen.
- Sichere und datenschutzfreundliche Authentifizierung von Nutzerinnen und Nutzern, soweit dies zur elektronischen Ausübung ihrer Rechte erforderlich ist.
- Erleichterte Durchsetzung von Nutzerrechten, etwa durch nutzerfreundliche Festlegung des anwendbaren Rechts und des Gerichtsstandes entsprechend dem im Verbraucherschutzrecht maßgeblichen Internationalen Privatrecht (Rom I- und II-Verordnungen; Urteil des Bundesgerichtshofs v. 2.3.2010 – VI ZR 23/09 – Klage gegen eine Internetveröffentlichung der New York Times).
- Besondere Regelungen zum Datenschutz bei Diensten, die sich an minderjährige Nutzerinnen und Nutzer richten.

Zusätzliche Anforderungen an die Zulässigkeit von Internetveröffentlichungen (im Unterschied zur herkömmlichen Veröffentlichung), nämlich

- Verpflichtung der Anbieter, Nutzerinnen und Nutzer auf mit der Veröffentlichung personenbezogener Daten verbundene Risiken hinzuweisen.
- Veröffentlichung personenbezogener Daten im Internet durch öffentliche Stellen grundsätzlich nur, soweit die entsprechende Rechtsgrundlage diese Veröffentlichungsform ausdrücklich mit einbezieht.
- Aufnahme von „Verfallsdaten“ für personenbezogene Daten bei deren Veröffentlichung im Internet, zumindest wenn Betroffene eigene Daten ins Netz stellen und ein solches Verfallsdatum setzen wollen.
- Gesetzliche Verpflichtung der Anbieter von Suchmaschinen, von Website-Anbietern verhängte „Indexierungsverbote“ und Verfallsdaten zu beachten.
- Pflicht zur Verwendung verfügbarer technischer Schutzmechanismen zur Gewährleistung der Datensicherheit, insbesondere zum Schutz vor dem unbefugten massenhaften Herunterladen von personenbezogenen Daten.

25

noch Anlage 6

Konferenz der Datenschutzbeauftragten des Bundes und der Länder
„Ein modernes Datenschutzrecht für das 21. Jahrhundert“

Die Bundesregierung wird darüber hinaus aufgefordert,

- im Rahmen internationaler Vereinbarungen die Anforderungen des Datenschutzes zur Geltung zu bringen.
- sich auf internationaler Ebene dafür einzusetzen, dass es zu verbindlichen Absprachen im Rahmen der Vereinten Nationen für ein möglichst hohes Datenschutzniveau und dessen Durchsetzung im Internet kommt.
- die internationalen Standardisierungsvorhaben damit zu verknüpfen.
- verstärkt Forschungsmittel zur Verbesserung des Datenschutzes in globalen Netzen vorzusehen, insbesondere zur Unterstützung und Stärkung der Rechte Einzelner im Cyberspace, z.B. zur Umsetzung von Verfallsdaten und zur Entwicklung eines „digitalen Radiergummis“ für Betroffene.

Auch im Internet muss die/der Einzelne ihr/sein Recht auf informationelle Selbstbestimmung durchsetzen können.

26

# 6. Eigenkontrolle der verantwortlichen Stellen

*Das gegenwärtige Datenschutzrecht ist vielfach noch geprägt durch Verbotsnormen, die selten zu Kontrollen führen und deren Sanktionen bei festgestellten Verstößen nicht ausreichen. Aufgrund sehr geringer Kontrolldichte führt dies zu erheblichen Vollzugsdefiziten. Ein modernes Datenschutzrecht muss deswegen die Elemente der Eigenkontrolle stärken. Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden, etwa als Vorteil im Wettbewerb, und nicht nur als von außen aufgezwungene Beschränkung. Daneben müssen interne Mechanismen bei den verantwortlichen Stellen entwickelt und gestärkt werden, die die Einhaltung des Datenschutzes sicherstellen, ohne dass es einer ständigen Kontrolle von außen bedarf.*

Die Konferenz der Datenschutzbeauftragten fordert das bestehende Datenschutzrecht um folgende Punkte zu ergänzen:

- Ausführungsgesetz zum Datenschutzaudit:

  Die Einführung eines freiwilligen bundesweiten Datenschutzaudits für Verfahren und Produkte der elektronischen Datenverarbeitung, mit dem die Einhaltung aller relevanten Datenschutzvorschriften bestätigt und darüber hinaus besonders datenschutzfreundliches Verhalten ausgezeichnet werden, wäre ein wirksames Mittel, Datenschutz zum Wettbewerbsvorteil zu machen.

- Aufstellung verbindlicher Datenschutzkonzepte:

  Eine Verpflichtung der verantwortlichen Stellen, für ihre Verarbeitung personenbezogener Daten ein Datenschutzkonzept zu entwickeln und der Aufsichtsbehörde auf Verlangen vorzulegen, würde diese zwingen, sich mit der Thematik umfassend für ihren jeweiligen Betrieb auseinanderzusetzen, Schwachstellen aufzudecken und entsprechende Vorkehrungen zu treffen. Hierzu sollte auch die bereits bestehende Verpflichtung zur Vorabkontrolle ausgebaut werden, insbesondere sollte festgeschrieben werden, dass die Durchführung der Vorabkontrolle schriftlich zu dokumentieren ist.

- Stärkung der behördlichen/betrieblichen Datenschutzbeauftragten:

  Die behördlichen und betrieblichen Datenschutzbeauftragten sind ein wichtiges Element der Eigenkontrolle, soweit sie ihre Aufgaben unabhängig, kompetent und mit ausreichenden Möglichkeiten wahrnehmen können. Deswegen sind Regelungen erforderlich, die zumindest
  - sie in ausreichendem Umfang von anderen Aufgaben freistellen,
  - ihre interne Beteiligung bei allen datenschutzrelevanten Vorgängen zwingend vorsehen,

noch Anlage 6



- sie als Ansprechpartnerinnen und -partner für Datenschutz nach innen und außen bekannt machen,
- die Unabhängigkeit und Qualität externer Datenschutzbeauftragter etwa durch Festlegung von Mindestanforderungen bei der Beauftragung stärken und
- eine Berichtspflicht einführen.

Mit diesen Maßnahmen kann die Verwirklichung des Datenschutzes in den verantwortlichen Stellen selbst verbessert und die externe Kontrolle entlastet werden. Das Audit würde den Datenschutz zum Wettbewerbsfaktor machen und auf diesem Wege stärken.

# 7. Datenschutzaufsicht

*Den Datenschutzaufsichtsbehörden kommt für die Verwirklichung eines effizienten Datenschutzes eine herausragende Rolle zu, da sie nicht nur die Einhaltung der datenschutzrechtlichen Bestimmungen kontrollieren, sondern die verantwortlichen Stellen im Vorfeld auch beraten und die Parlamente und die Öffentlichkeit über datenschutzrechtliche Probleme und Lösungswege informieren. Die Stärkung der Aufsichtsbehörden ist deswegen zugleich auch eine Verbesserung des Datenschutzes. Es gibt neben der vielfach unzureichenden personellen Ausstattung aber weitere Punkte, die eine wirkungsvolle Datenschutzaufsicht beeinträchtigen.*

Die Datenschutzbeauftragten des Bundes und der Länder halten folgende gesetzgeberische Maßnahmen für erforderlich:

- Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten ist mit der EG-Datenschutzrichtlinie nicht vereinbar. Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.
- Das mit dem Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14.08.2009 (BGBl. I S. 2814) eingeführte Anordnungsrecht in § 38 Abs. 5 BDSG ist zwar ein erster Schritt. Dieses muss jedoch effektiver ausgestaltet und den üblichen Grundsätzen des Verwaltungsvollzugs angepasst werden.
- Mitwirkungspflicht der kontrollierten Stelle gegenüber Kontrollen der Aufsichtsbehörde:

  § 38 Abs. 4 BDSG sieht bislang nur das Recht der Aufsichtsbehörde vor, die zu kontrollierende Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Ohne aktive Mitwirkung der zu kontrollierenden Stelle, wie sie etwa § 24 Abs. 4 BDSG für die Tätigkeit des Bundesbeauftragten vorsieht oder § 5 des Gesetzes zur Bekämpfung der Schwarzarbeit und illegalen Beschäftigung, gehen solche Kontrollen aber oft ins Leere, wenn z. B. vor Ort niemand da ist, der Fragen beantwortet, die Datenverarbeitungssysteme und -verfahren erläutert oder die technischen Voraussetzungen für wirksame Prüfungen schafft.
- Ausweitung der Informationspflicht bei Datenpannen auf öffentliche Stellen.

noch Anlage 6

Konferenz der Datenschutzbeauftragten des Bundes und der Länder
„Ein modernes Datenschutzrecht für das 21. Jahrhundert“

- Anordnungsbefugnisse auch für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit:

  Durch die jüngsten Gesetzesänderungen haben zwar die in § 38 BDSG erwähnten Aufsichtsbehörden ein Anordnungsrecht bei Datenschutzverstößen erhalten, es fehlt aber eine vergleichbare Regelung für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in den Bereichen, in denen er nicht-öffentliche Stellen nach dem Telekommunikationsgesetz und dem Postgesetz kontrolliert.

- Ausdehnung der Zeugnisverweigerungsrechte und Beschlagnahmeschutzvorschriften auf Informationen und Unterlagen, die die Aufsichtsbehörden bei Berufsgeheimnisträgerinnen und -trägern erlangt haben:

  Die gesetzlich vorgesehene Datenschutzkontrolle von Berufsgeheimnisträgerinnen und -trägern durch die staatlichen Aufsichtsbehörden wird von diesen teilweise mit der Begründung verweigert, dort erlangte Kenntnisse und Unterlagen unterlägen bei den Aufsichtsbehörden nicht in gleicher Weise dem strafverfahrensrechtlichen Zeugnisverweigerungsrecht und Beschlagnahmeschutz wie bei den Berufsgeheimnisträgerinnen und -trägern selbst. Deswegen sei eine solche Kontrolle nicht zulässig. Aus diesem Grunde bedarf es entsprechender Vorschriften im Strafgesetzbuch und im Datenschutzrecht, wie sie für externe betriebliche Datenschutzbeauftragte schon geschaffen wurden.

- Strafantragsbefugnis für die Datenschutzaufsichtsbehörden in § 205 StGB:

  Nicht selten erhalten die Aufsichtsbehörden Kenntnis von Datenschutzverstößen, die zugleich eine Strafbarkeit nach den §§ 201 - 204 StGB begründen können. In der Praxis scheitert die Strafverfolgung aber zum Teil daran, dass der nach § 205 StGB erforderliche Strafantrag nicht gestellt wird. Deswegen sollte auch den Aufsichtsbehörden diese Möglichkeit eingeräumt werden, wie in § 44 BDSG für den nicht-öffentlichen Bereich bereits geschehen.

Durch diese Maßnahmen würden die Möglichkeiten der Aufsichtsbehörden deutlich gestärkt, ihre Kontrollaufgaben wirksam wahrzunehmen.

30

## 8. Sanktionen

*Die erheblichen Vollzugsdefizite im Datenschutz sind unter anderem auch darauf zurückzuführen, dass Verstöße gegen datenschutzrechtliche Bestimmungen vielfach folgenlos bleiben. Gründe hierfür sind zum einen nicht ausreichende Sanktionsmöglichkeiten und zum anderen praktische Probleme bei der Verhängung von Bußgeldern oder der Strafverfolgung. So sind z. B. immer noch wichtige Datenschutzvorschriften nicht bußgeldbewehrt, Haftungsansprüche werden nur selten geltend gemacht, weil die Anspruchsteller nicht nur den Datenschutzverstoß nachweisen müssen, sondern auch ein Verschulden der verantwortlichen Stelle und eine konkrete Schadenshöhe. Außerdem fallen aufgrund fehlender Zuständigkeitsregelungen oft Datenschutzaufsicht und zuständige Bußgeldbehörde auseinander. Deswegen sind inhaltliche und verfahrensrechtliche Änderungen erforderlich, damit Daten verarbeitende Stellen aufgrund erhöhten Risikos von sich aus intensiver auf die Einhaltung der geltenden Datenschutzvorschriften achten.*

Um die Sanktionsmöglichkeiten und ihren Vollzug effizienter zu gestalten, hält die Konferenz der Datenschutzbeauftragten des Bundes und der Länder folgende Maßnahmen für erforderlich:

- Einführung einer Gefährdungshaftung auch für nicht-öffentliche Stellen:
  - Nach § 8 Abs. 1 BDSG besteht eine verschuldensunabhängige Haftung für Datenschutzverstöße nur bei öffentlichen Stellen. Da die Gefährdung des Grundrechts auf informationelle Selbstbestimmung aber bei nicht-öffentlichen Stellen in mindestens gleicher Weise besteht, sollte auch für diesen Bereich eine vergleichbare Gefährdungshaftung eingeführt werden. Die Geltendmachung von Schadensersatzansprüchen scheitert vielfach daran, dass die Betroffenen zwar einen Datenschutzverstoß nachweisen können, aber kein Verschulden.
  - Konkretisieren sich in der elektronischen Datenverarbeitung immanente Risiken, kann dies nicht zu Lasten der Betroffenen gehen.
- Einführung eines pauschalierten Schadensersatzes für Datenschutzverstöße:

  Nach geltendem Recht kann nach einem Datenschutzverstoß nur dann Schadensersatz verlangt werden, wenn der/dem Betroffenen ein konkret bezifferbarer Schaden entstanden ist, den sie/er nachweisen muss. Immaterielle Schäden können nach § 8 Abs. 2 BDSG nur bei schweren Verletzungen des Persönlichkeitsrechts und nur gegenüber öffentlichen Stellen geltend gemacht werden. Allerdings ist dies im Einzelfall u. U. auch nach den allgemeinen Haftungsregelungen des Bürgerlichen Gesetzbuchs möglich.

noch Anlage 6



Ein pauschalierter Anspruch (unbeschadet weiterer Ansprüche bei nachweisbar höheren Schäden) würde dieses Problem lösen und zugleich die Anstrengungen der verantwortlichen Stellen erhöhen, von sich aus Verletzungen des Datenschutzes zu verhindern.

- Anspruch der Betroffenen gegen die verantwortliche Stelle, auf die Beseitigung von durch unrichtige oder unrechtmäßige Datenübermittlung entstandene negative Folgen hinzuwirken:

  Werden unrechtmäßige oder unrichtige Daten an Dritte übermittelt, kann das für die Betroffenen fatale Folgen haben. Falsche Angaben einer Kreditauskunftei (etwa aufgrund einer Verwechslung oder eines unrichtigen Datenbestandes) können dazu führen, dass den Betroffenen Kredit-, Handyverträge oder Konten gekündigt werden. Weisen diese den Irrtum nach, berichtigt die Kreditauskunftei zwar ihren Datenbestand, mit den eingetretenen Folgen bleiben die Betroffenen aber allein und müssen selbst versuchen, die Kündigungen rückgängig zu machen oder andere Folgen zu beseitigen. Die vorgeschlagene Maßnahme würde hier die Verursacherinnen und Verursacher in die Pflicht nehmen. Eine solche Regelung würde darüber hinaus das Eigeninteresse von Auskunfteien steigern, die Richtigkeit ihres Datenbestandes zu überprüfen und Irrtümer zu vermeiden.

- Erweiterung der Bußgeldtatbestände, insbesondere für
  - unbefugtes Nutzen von Daten,
  - unzulässige Beobachtung, Registrierung und Zweckänderung durch automatisierte Verfahren (z.B. Videoüberwachung),
  - das Unterlassen von technisch-organisatorischen Maßnahmen:

    Noch immer gibt es eine Reihe von wichtigen Datenschutzbestimmungen, deren Nichtbeachtung nicht mit einem Bußgeld geahndet werden kann. Hierzu gehören insbesondere das unbefugte Nutzen von Daten und die Gefährdung elektronischer Datenverarbeitungssysteme durch Unterlassen der erforderlichen Schutzmaßnahmen, die etwa in § 9 BDSG und der Anlage dazu vorgesehen sind. Diese Lücken sind im Interesse eines effizienten Datenschutzes zu schließen.

- Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten konzentrieren:

  Die Datenschutzgesetze enthalten zwar eine Vielzahl von Bußgeldtatbeständen, vielfach aber keine eigenständige Zuständigkeitsregelung für deren Verfolgung, sodass insoweit die allgemeinen Regelungen des Ordnungswidrigkeitenrechts gelten. Deswegen sind häufig weder die Datenschutzaufsichtsbehörde, die den Datenschutzverstoß festgestellt hat, noch eine andere zentrale, landes- oder bundesweit agierende Stelle zuständig, sondern die jeweils fachlich zuständige oberste Landes- bzw. Bundesbe-

hörde, die aber wegen der geringen Fallzahlen häufig ihre Zuständigkeit für die Ahndung von Datenschutzverstößen gar nicht kennt, keine Erfahrung im Datenschutz hat und keine Übung in der Durchführung von Ordnungswidrigkeitenverfahren. Deswegen kommt es in vielen Fällen zu keiner Verfolgung von datenschutzrechtlichen Ordnungswidrigkeiten, obwohl die Voraussetzungen dafür vorliegen.

- Verfolgung von datenschutzrechtlichen Straftaten auch von Amts wegen, wenn ein besonderes öffentliches Interesse gegeben ist:

  Nach geltendem Recht setzt die Verfolgung von Straftaten im Datenschutzrecht einen Antrag voraus, den nur die oder der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit oder die Datenschutzaufsichtsbehörde stellen können. Es häufen sich die Fälle, in denen Strafverfolgungsbehörden, die von sich aus auf entsprechende Straftaten gestoßen sind, eine/einen Antragsberechtigte/Antragsberechtigten suchen müssen, um die Vergehen verfolgen zu können. Deswegen sollte in den Fällen, in denen ein besonderes öffentliches Interesse an einer Strafverfolgung gegeben ist, eine Verfolgung auch von Amts wegen möglich sein.

Durch die aufgeführten Maßnahmen könnte das datenschutzrechtliche Sanktionssystem sehr viel wirkungsvoller auf Datenschutzverstöße reagieren. Damit ließen sich die Vollzugsdefizite verringern, weil die betroffenen Stellen größere Anstrengungen zeigen würden, Datenschutzverstöße gar nicht erst entstehen zu lassen.

noch Anlage 6

Konferenz der Datenschutzbeauftragten des Bundes und der Länder
„Ein modernes Datenschutzrecht für das 21. Jahrhundert“

## 9. Vereinfachung und bessere Lesbarkeit des Gesetzes

*Das BDSG ist in Aufbau, Wortlaut und Regelungstechnik kaum noch verständlich und nachvollziehbar. Selbst für Fachleute ist es inzwischen schwierig, für konkrete Sachverhalte das Recht korrekt anzuwenden. Normale Anwender, die nicht über eigene Rechtsabteilungen oder spezialisierte Fachanwälte verfügen, sind hier vielfach überfordert.*

*Auch für die Bürgerinnen und Bürger, die sich selbst anhand des Gesetzes über ihre Rechte und die Möglichkeiten, diese durchzusetzen, informieren wollen, werden fast unüberwindbare Verständnishürden aufgebaut. Die Vollzugsdefizite im Datenschutz gehen zu einem Teil auf die Unverständlichkeit der Regelungen zurück. Deswegen muss das BDSG einfacher und verständlicher gestaltet werden. Hierzu können auch Änderungen bei den Definitionen gehören, die zusätzliche Spezialvorschriften entbehrlich machen.*

Neben bereits aufgeführten Maßnahmen, wie z. B. einer möglichst weitreichenden Vereinheitlichung der Vorschriften für den öffentlichen und den nichtöffentlichen Bereich, hält die Konferenz der Datenschutzbeauftragten des Bundes und der Länder folgende Punkte für erforderlich:

- Neue Definition des Begriffs „Verarbeiten“, die sowohl das Erheben wie das Nutzen von personenbezogenen Daten umschließt:

  Die derzeitige Begrifflichkeit des BDSG umfasst gesondert das „Erheben“ (§ 3 Abs. 3), das „Verarbeiten“ (§ 3 Abs. 4) und das „Nutzen“ (§ 3 Abs. 5) von personenbezogenen Daten. Aufgrund dieser unterschiedlichen Terminologie werden in zahlreichen Bestimmungen des BDSG immer alle drei Begriffe hintereinander aufgezählt, was Lesbarkeit und Verständnis beeinträchtigt. Die Europäische Datenschutzrichtlinie definiert „Verarbeiten“ hingegen so (Art. 2b), dass „Erheben“ und „Benutzen“ mit umfasst werden.

- Einheitliche Anwendung des Datenschutzrechts für alle Formen der Verarbeitung personenbezogener Daten:

  Im Gegensatz zum öffentlichen Bereich gilt das BDSG im nichtöffentlichen Bereich nur für den Einsatz von Datenverarbeitungsanlagen und nicht automatisierte Dateien, nicht aber für personenbezogene Daten in normalen Papierakten. Diese Unterscheidung ist im Blick auf die Schutzziele nicht sinnvoll und verliert aufgrund des technologischen Fortschritts zunehmend an Bedeutung. Sie sollte aufgegeben werden, was das Gesetz auch vereinfachen würde.

34

- Aufnahme von „genombezogenen Daten“ in die Definition der besonderen Arten personenbezogener Daten:

  Personenbezogene Daten, die sich aus genetischen Untersuchungen und Analysen ergeben, sind besonders sensibel, aber durch die Definition der besonderen Arten personenbezogener Daten nur so weit erfasst, wie es sich dabei um Gesundheitsdaten handelt. Der besondere Schutz für diese Datenkategorie sollte auf alle genombezogenen Daten erweitert werden, zumindest soweit sie nicht offensichtlich sind, wie etwa das Geschlecht.

- Definition der „öffentlich zugänglichen Daten“ und spezielle Regelungen für den Umgang damit:

  Die Datenschutzgesetze des Bundes und der Länder sehen vielfach vor, dass für den Umgang mit personenbezogenen Daten, die öffentlich zugänglich sind oder aus öffentlich zugänglichen Quellen stammen, geringere Anforderungen gelten oder die Schutzvorschriften gar nicht zur Anwendung kommen. Dies muss mit Blick auf das Internet überdacht werden. Zum einen ist der Begriff „öffentlich zugänglich“ einschränkend zu definieren, etwa indem eine entsprechende Zweckbestimmung durch den Betroffenen selbst oder aufgrund gesetzlicher Regelung (öffentliche Register) erforderlich ist, zum anderen bedarf es spezieller Regelungen zur Interessensabwägung und zur Zweckbindung.

Die vorgeschlagenen Maßnahmen würden das Datenschutzrecht lesbarer und verständlicher machen und zur Vereinfachung beitragen.

**Anlage 7**

## Europäische Datenschutzkonferenz vom 23. bis 24. April 2009 in Edinburgh

## Erklärung zur Führungsrolle und Zukunft des Datenschutzes in Europa

Europa hat eine lange und stolze Geschichte von Standards und Gesetzgebung im Bereich des Datenschutzes. Einige davon wurden im Laufe der Zeit geändert und andere werden unter Beobachtung bleiben. Die Gesetzgebung folgt immer dem technischen und sozialen Fortschritt und es ist für die Datenschutzbehörden eine Herausforderung, mit diesen Entwicklungen Schritt zu halten und angesichts dieser sich schnell ändernden Umstände die Gesetze anzuwenden und eine Strategie zu entwickeln.

Datenschutzrechtliche Standards und Gesetzgebung entwickeln sich auch zügig in den restlichen Teilen der Welt und Europa spielte aufgrund seiner beratenden und unterstützenden Tätigkeit eine wichtige Rolle in einigen Ländern. Obwohl die bestehenden Standards und Gesetzgebungen Unterschiede in bestimmten Bereichen aufweisen können, zielen sie letzten Endes doch alle auf den Schutz personenbezogener Daten und die Rechte und Freiheiten der Einzelnen ab.

Die Konferenz verpflichtet sich, einen Beitrag für die Entwicklung des Datenschutzes in Europa zu leisten und dafür zu sorgen, dass aus den Erfahrungen der europäischen Länder Nutzen für die weltweite Diskussion über den Datenschutz gezogen wird. Dazu gehört auch die bessere Umsetzung und Durchsetzung des bestehenden Rechtsrahmens.

Die europäischen Datenschutzbeauftragten stehen zu ihrer Führungsrolle in der Zukunft. Dementsprechend erwartet die Konferenz, dass die Datenschutzbeauftragten einen konstruktiven Beitrag zu den laufenden Arbeiten und Initiativen leisten, die darauf abzielen, die Diskussion über die Zukunft des Datenschutzes in Europa und insbesondere über den zukünftigen Rechtsrahmen voranzubringen.

Die Konferenz wird sich weiterhin für die Notwendigkeit von hohen Datenschutzstandards in allen Lebensbereichen einsetzen, insbesondere in Bezug auf technologische Entwicklungen, die Online-Welt und Strafverfolgungsmaßnahmen.

Die Konferenz unterstützt die Entwicklung und Verbesserung einer umfassenden Gesetzgebung zum Datenschutz, die

- die Grundrechte und Freiheiten gewährleistet und fördert;
- auf bestehenden Datenschutzgrundsätzen aufbaut;
- Wert darauf legt, dass die angestrebten Ergebnisse in der Praxis auf effektive Art und Weise erreicht werden;
- Organisationen ermutigt, beste Praktiken zu übernehmen, wie etwa „privacy by design“ (eingebauter Datenschutz);
- die Risiken schädlicher Auswirkungen angeht, denen der Einzelne und die Gesellschaft insgesamt ausgesetzt sind;
- nicht zu rechtfertigende Belastungen vermeidet und
- für eine effektive Durchsetzung sorgt.

Die Konferenz ruft alle auf, die an Diskussionen über Strategien und Gesetze zum Datenschutz beteiligt sind, sich mit den Gemeinsamkeiten statt mit den Unterschieden verschiedener Regelwerke und Rahmenwerke zu befassen und nach Wegen zur Förderung globaler Lösungen zu suchen. Indem sie die Erfahrungen der europäischen Länder in die weltweite Debatte mit einbringt, ermutigt die Konferenz zu einem Geist der Zusammenarbeit, der vollständig mit der Förderung der Grundrechte und Freiheiten im Einklang steht.

Mit dieser Erklärung nimmt die Konferenz zur Kenntnis, dass sich die Datenschutzlandschaft sowohl innerhalb als auch außerhalb Europas weiterentwickelt. Sie sieht auch die Notwendigkeit, unsere Arbeit zur Förderung des Datenschutzes und der Datenschutzstandards fortzusetzen, indem wir uns an die Welt anpassen, in der wir leben.

**Anlage 8**

## Entschließung der Frühjahrskonferenz 2009 der Europäischen Datenschutzbeauftragten

## zu bilateralen und multilateralen Abkommen zwischen europäischen Staaten und Drittstaaten im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Die Datenschutzstandards in bilateralen und multilateralen Abkommen, die europäische Staaten mit Drittstaaten im Bereich der polizeilichen und justiziellen Zusammenarbeit geschlossen haben, weisen große Unterschiede auf.

Die geltenden Rechtsrahmen, die Konvention 108, ihre Protokolle und der Rahmenbeschluss 2008/977/JHA über den Schutz personenbezogener Daten gewährleisten ein besonderes datenschutzrechtliches Regelwerk für den Austausch personenbezogener Daten.

Angesichts dieser Tatsache weist die Europäische Datenschutzkonferenz darauf hin, dass diese großen Unterschiede das von den europäischen Staaten verfolgte Ziel, nämlich die Schaffung eines möglichst einheitlichen und effektiven Datenschutzes für alle Personen, gefährden.

Die Konferenz fordert daher alle europäischen Staaten auf, sicherzustellen, dass beim Abschluss internationaler Abkommen geltende Datenschutzstandards eingehalten werden. In diesem Zusammenhang setzt sich die Konferenz nachdrücklich für die Entwicklung und die anschließende Aufnahme solcher datenschutzrechtlicher Standardklauseln in diesen Abkommen ein.

**Anlage 9**

## Entschließung der Frühjahrskonferenz 2010 der Europäischen Datenschutzbeauftragten

## zu dem geplanten Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Datenschutzstandards im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Auf der Grundlage des Abschlussberichts der sogenannten High Level Contact Group wollen Vertreter der Europäischen Union und der Vereinigten Staaten von Amerika Verhandlungen über ein Abkommen zu Datenschutzstandards für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen aufnehmen.

Die Europäischen Datenschutzbeauftragten begrüßen dieses Vorhaben sehr. Sie hegen große Hoffnung, dass sich die Europäische Union und die Vereinigten Staaten von Amerika durch dieses Abkommen verpflichten werden, beim Austausch personenbezogener Daten in Strafsachen ein hohes Datenschutzniveau einzuhalten und dadurch ein Beispiel für andere internationale Abkommen zum Datenaustausch im Bereich der Strafverfolgung geben.

Die europäischen Datenschutzbeauftragten messen dem Abkommen große Bedeutung bei, denn angesichts von internationalem Terrorismus und grenzüberschreitender Kriminalität werden die Herausforderungen an die internationale Kooperation von Strafverfolgungsbehörden aller Voraussicht nach weiter anwachsen und damit auch die Bedingungen für den internationalen Datenaustausch zwischen den Sicherheitsbehörden zunehmend auf der politischen Tagesordnung stehen.

In diesem Sinne fordert die Europäische Datenschutzkonferenz die Europäische Union auf, sich für ein hohes Datenschutzniveau stark zu machen und – mittels dieses Abkommens – unverrückbare Prinzipien – insbesondere eine enge Zweckbindung der übermittelten Daten, eine hohe Datensicherheit, unabhängige Datenschutzaufsichtsbehörden sowie das Auskunftsrecht und den gerichtlichen Rechtsschutz für alle Betroffenen, unabhängig von ihrer Nationalität oder ihres Aufenthaltslandes – auch bei einem Datenaustausch mit den USA auf effektive Weise sicherzustellen.

Nähere Einzelheiten zu den Erwartungen und Hoffnungen der Europäischen Datenschutzkonferenz finden Sie in dem gemeinsamen Beitrag der WPPJ und der Artikel 29-Arbeitsgruppe zu der öffentlichen Konsultation der Europäischen Kommission in dieser Angelegenheit.

**Anlage 10**

## Entschließung zum Einsatz von Körperscannern für die Sicherheit an Flughäfen angenommen von der Europäischen Datenschutzkonferenz am 29./30. April 2010 in Prag

Der gescheiterte Anschlag auf den Delta Flug 253 Amsterdam – Detroit am 25. Dezember 2009 entfachte eine weltweite Diskussion bei Regierungen und Sicherheitsbehörden darüber, wie die Sicherheit auf Flughäfen erhöht werden könnte und ob Körperscanner zur Erleichterung der Kontrollen der Flugpassagiere, bevor sie an Bord gehen, eingesetzt werden sollten. Der Einsatz solcher Körperscanner und das Durchleuchten des gesamten menschlichen Körpers kann eine schwere Verletzung des Rechts des Passagiers auf Schutz der Privatsphäre und auf Datenschutz darstellen. Daher sollten Datenschutzprinzipien und -sicherungsmaßnahmen ebenso berücksichtigt werden wie „Privacy by Design" wenn der Einsatz von Körperscannern in Erwägung gezogen wird.

Die Notwendigkeit der Verarbeitung ist eines der Datenschutzprinzipien, das berücksichtigt werden muss. Es ist immer noch nicht klar, ob sich mit diesen Geräten wirklich eine höhere Sicherheit an Flughäfen erreichen lässt. Vor ihrem Einsatz muss auch die Frage hinsichtlich ihrer Effektivität und ihrer Auswirkungen auf die Gesundheit der Passagiere in Betracht gezogen werden.

Vor dem Hintergrund des aktuellen Diskussionsstandes sieht die Europäische Datenschutzkonferenz mit Besorgnis, dass neue Geräte eingesetzt werden, die nicht den Datenschutzstandards entsprechen. Deshalb möchte die Konferenz die Notwendigkeit einer wissenschaftlich fundierten und koordinierten Diskussion dieses Themas betonen.[1] Alle Interessengruppen, wie Wissenschaftler, Technikexperten, Fachleute aus den Bereichen Gesundheit und Datenschutz sollten angehört werden, um zu einer angemessenen Bewertung der anstehenden Punkte zu gelangen. Insbesondere sind vor einer voreiligen Entscheidung zu dem Einsatz von Körperscannern die folgenden Aspekte anzusprechen.

1. Ist der Einsatz von Körperscannern an Flughäfen für die Flugsicherheit notwendig und wenn ja, in welchen Ausmaß? Zu dieser Frage sind detaillierte Studien unter Einbeziehung wissenschaftlicher Methoden durchzuführen. Die Nützlichkeit der Körperscanner sollte auf einer soliden empirischen Grundlage bewiesen werden. Bis heute gibt es ernsthafte Zweifel hinsichtlich der erweiterten Fähigkeiten der Körperscanner mit Blick auf die Detektierbarkeit explosiver Stoffe, wie zum Beispiel kleiner Mengen von Flüssigkeiten oder anderer Stoffen von geringer Dichte. Ist im Vergleich mit anderen Methoden zur Personenkontrolle wie dem Gang durch Metalldetektoren, Handscannern oder Leibesvisitationen ein Zugewinn an Sicherheit zu verzeichnen? Falls es weniger einschneidende Methoden zur Erreichung des gleichen zusätzlichen Sicherheitsniveaus gibt,[2] dann sollten diese genutzt werden.

2. Gibt es angemessene Schutzmaßnahmen, die die Privatsphäre der durch Körperscanner durchleuchteten Personen gewährleisten? Technische Maßnahmen müssen sicherstellen, dass die personenbezogenen Daten der Reisenden weder gespeichert noch weitergeleitet werden. Sobald der Passagier für sicher erklärt wurde, sollten die Bilder sofort gelöscht werden. Schematische Darstellungen der Körper von Personen sind überaus datenschutzfreundlich. Daher könnte dieser Methode, Körper auf Bildschirmen zu zeigen, der Vorzug gegeben werden. Falls intime Details von Personen, wie z. B. medizinische Hilfsmittel oder künstliche Körperteile angezeigt werden, sollten sie nur für die diensthabende Person zu sehen sein. Die mit dem Ansehen der vom Körperscanner angezeigten Bilder befassten Personen dürfen nicht mit den Personen, die an weiteren Kontrollen beteiligt sind, identisch sein. Sie müssen ihre Aufgaben in Einrichtungen wahrnehmen, die ihnen keine Kommunikation mit den anderen Kontrolleuren erlauben, und sie dürfen nicht in der Lage sein, die Passagiere zu sehen. Außerdem sollten Körperscanner nur eingesetzt werden, nachdem eine Datenschutz-Verträglichkeitsprüfung (PIA) durchgeführt wurde, aus der hervorgehen sollte, dass die hier erwähnten Grundsätze mit einbezogen wurden.

Nur wenn ein fairer Ausgleich zwischen der Effektivität und Notwendigkeit dieser neuen technologischen Geräte einerseits und der Auswirkung auf die Privatsphäre der Flugpassagiere andererseits geschaffen wird, könnte der Einsatz von Körperscannern aus datenschutzrechtlicher Sicht als angemessen und als ein geeignetes Mittel für die Sicherheitsdurchleuchtung betrachtet werden.

Deshalb ruft die Europäische Datenschutzkonferenz alle Entscheidungsträger aus ganz Europa dazu auf, gründlich über die Auswirkungen der Körperscanner auf die Grundrechte der Reisenden nachzudenken, bevor sie ihren Einsatz am Flughafen beschließen.

---

[1] Die Art. 29 WP hat am 11. Februar 2009 ein Arbeitspapier zu Körperscannern angenommen. Dieses Arbeitspapier und der Begleitbrief an die Europäische Kommission ist auf folgender Webseite zu finden: http://ec.uropa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2009_05_11_letter_chairman_art29wp_daniel_calleja_dgtren_en.pdf http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2009_05_11_annex_consultation_letter_chairman_art29wp_daniel_calleja_dgtren_en.pdf

[2] wie z. B. Handscanner oder Spürhunde

Es sollten nur Geräte eingesetzt werden, in die datenschutzfreundliche Technologien eingebaut wurden und die einen angemessenen Ausgleich zwischen der Notwendigkeit nach erhöhter Sicherheit und dem Recht auf Schutz der Privatsphäre und des Datenschutzes schaffen. Die Datenschutzbehörden sollten weiterhin in den Entscheidungsprozess einbezogen werden, insbesondere während der Probe- und Testphasen, vor allem durch Vorabprüfung von Körperscannersystemen (falls nach nationalem Recht anwendbar) und durch Kontrollmöglichkeiten mit Blick auf das Funktionieren der Geräte nach deren Installation.

Die Passagiere sollten vor der Kontrolle durch Körperscanner angemessen über diese Geräte und über ihre Datenschutzrechte informiert werden. Zu diesem Zweck sollten die Flughafenbehörden eng mit ihren jeweils zuständigen Datenschutzbehörden zusammenarbeiten um sicherzustellen, dass entsprechende Merkblätter den rechtlichen Anforderungen entsprechen.

**Anlage 11**

## Entschließung der 31. Internationalen Datenschutzkonferenz vom 4. bis 6. November 2009 in Madrid über Internationale Standards zum Schutz der Privatsphäre

– Übersetzung –

Berücksichtigend, dass:

- die 30. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in Strassburg einstimmig den Beschluss über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Ausarbeitung einer gemeinsamen Entschließung zur Abfassung Internationaler Richtlinien zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten fasste;
- die Konferenz die „Agencia Española de Protección de Datos“ (im Folgenden: die spanische Datenschutzbehörde, d. Übers.) in ihrer Eigenschaft als Koordinatorin der 31. Internationalen Konferenz damit beauftragte, eine Arbeitsgruppe, die sich aus den interessierten Datenschutzbehörden zusammensetzen sollte, mit dem Ziel zu bilden, einen Gemeinsamen Vorschlag zur Abfassung Internationaler Standards zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten auszuarbeiten;
- die spanische Datenschutzbehörde gemäß diesem Auftrag eine Arbeitsgruppe bildete und die Arbeiten zur Erstellung eines Gemeinsamen Vorschlags für die Abfassung Internationaler Standards zum Schutz der Privatsphäre und der personenbezogenen Daten förderte und koordinierte;
- die Arbeitsgruppe den Gemeinsamen Vorschlag zur Abfassung Internationaler Standards zum Schutz der Privatsphäre und der personenbezogenen Daten insbesondere auf der Grundlage der Gemeinsamkeiten verschiedener juristischer Texte, Standards und Empfehlungen mit internationaler Reichweite, die in unterschiedlichen geografischen, wirtschaftlichen oder rechtlichen Anwendungsgebieten auf einen breiten Konsens gestoßen waren, entwickelte;
- bei der Erarbeitung des Gemeinsamen Vorschlags davon ausgegangen wurde, dass diese gemeinsamen Prinzipien und Ansätze Wertvolles zur Förderung des Schutzes der Privatsphäre und der persönlichen Information beitragen könnten und dass die Arbeitsgruppe die Erweiterung dieser Ansätze durch spezifische Lösungen und Standards anstrebte, die trotz der bestehenden Differenzen zwischen den vorhandenen Modellen zum Datenschutz und zum Schutz der Privatsphäre als anwendbar betrachtet wurden.

Im Einklang damit beschließt die Konferenz Folgendes:

1. Sie begrüßt den Gemeinsamen Vorschlag zur Abfassung der Internationalen Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung von personenbezogenen Daten, die diesem Beschluss als Anlage beiliegt. Der Gemeinsame Vorschlag belegt zum angemessenen Zeitpunkt die Möglichkeit der Festlegung solcher Standards als einen neuen Schritt in Richtung auf die Ausarbeitung eines international verbindlichen Instruments.
2. Sie bestätigt, dass der Gemeinsame Vorschlag Grundsätze, Rechte, Verpflichtungen und Verfahrensweisen enthält, die zum Datenschutz und zum Schutz der Privatsphäre von allen Rechtssystemen angestrebt werden sollten. Auf diese Weise könnte die Verarbeitung personenbezogener Daten im öffentlichen und privaten Sektor weltweit einheitlicher erfolgen, und zwar:
   a. fair, rechtmäßig und angemessen im Hinblick auf bestimmte explizite und legitime Zwecke;
   b. auf der Grundlage einer transparenten Politik, mit angemessenen Informationen für die Interessierten und ohne willkürliche Diskriminierungen, die diesen Grundsätzen widersprächen;
   c. die Genauigkeit, Vertraulichkeit und Sicherheit der Daten sowie die Legitimität der Datenverarbeitung und die Rechte der Betroffenen auf Einsehen, Richtigstellung und Löschung der Daten sowie auf Widerspruch gegen eine bestimmte Datenverarbeitung gewährleistend;
   d. unter Anwendung des Haftungsprinzips, einschließlich der Schadenshaftung, was auch die Datenverarbeitung durch Dienstleistungserbringer, die im Auftrag des Verantwortlichen handeln, einschließt;
   e. mit geeigneteren Garantien, wenn es sich um sensible Daten handelt;
   f. mit der Gewährleistung, dass international übertragene Daten unter dem in den genannten Standards vorgesehenen Schutz stehen;
   g. indem die Datenverarbeitung unter die Kontrolle von unabhängigen und unparteiischen Aufsichtsbehörden gestellt wird, die über die angemessenen Befugnisse und Ressourcen verfügen müssen und zur Zusammenarbeit verpflichtet sind;
   h. durch die Schaffung eines neuen und modernen Bezugsrahmens proaktiver Maßnahmen, deren Ziel insbesondere die Vorbeugung und Feststellung von Verstößen ist und die auf der Ernennung von Beauftragten für den Datenschutz und den Schutz der Privatsphäre, wirksamen Audits und Datenschutz-Folgenabschätzungen beruhen.

3. Sie ermutigt die bei der Internationalen Konferenz akkreditierten Beauftragten für den Datenschutz und den Schutz der Privatsphäre zur Verbreitung des Gemeinsamen Vorschlags zur Abfassung Internationaler Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten.

4. Sie beauftragt die für die Organisation der 31. und 32. Internationalen Konferenzen Verantwortlichen mit dem Aufbau einer Kontaktgruppe, an der die interessierten Beauftragten für den Datenschutz und den Schutz der Privatsphäre teilnehmen sollen. Diese Gruppe soll folgende Aufgaben in Angriff nehmen:

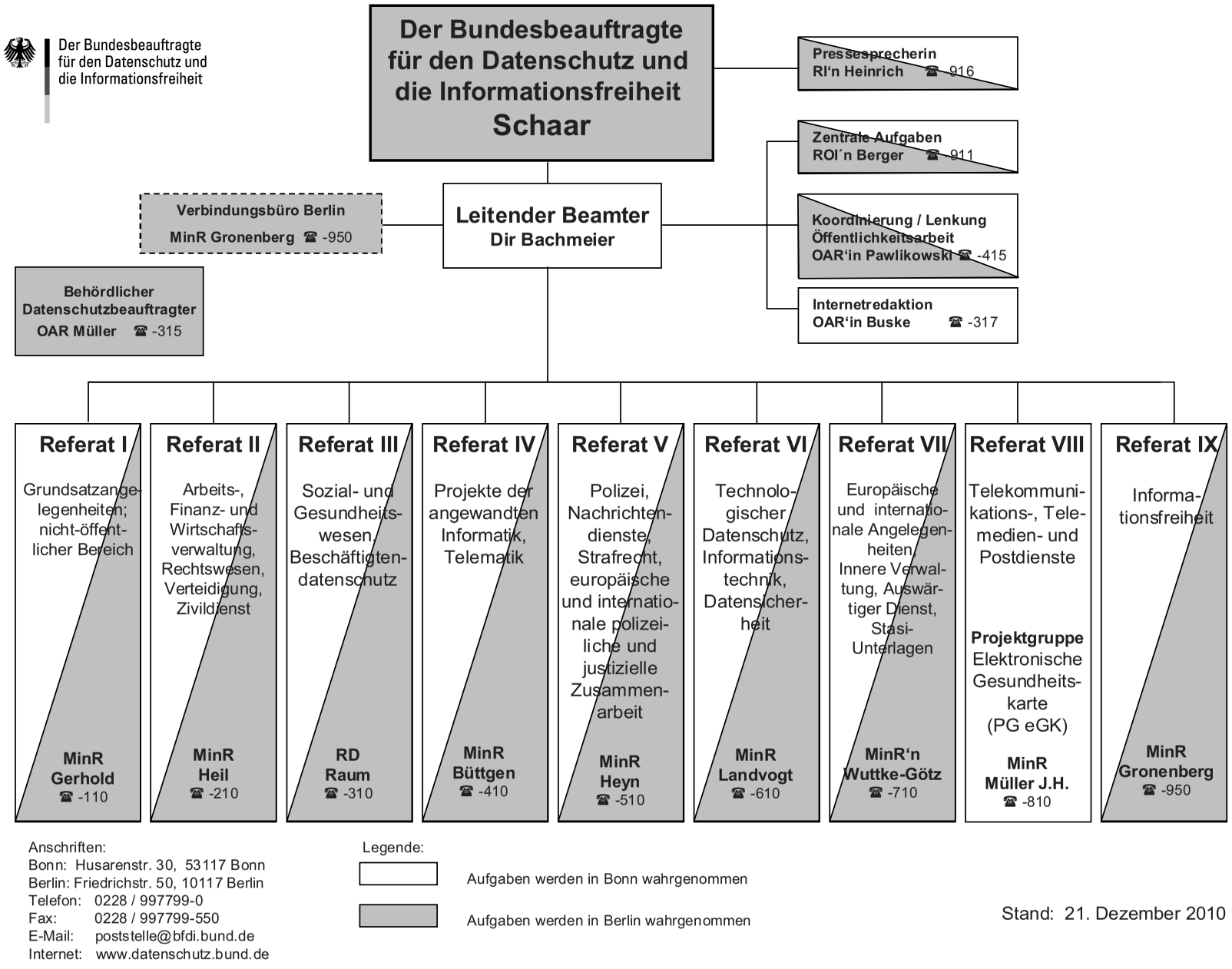
   a. Die Förderung und die Verbreitung des Gemeinsamen Vorschlags unter privaten Instanzen, Experten sowie in- und ausländischen öffentlichen Stellen, insbesondere unter den in der Erklärung von Montreux aufgeführten Institutionen und Organisationen als Grundlage für die zukünftige Arbeit an einem verbindlichen universellen Abkommen; sowie

   b. die Untersuchung und Information über weitere Möglichkeiten der Verwendung des Gemeinsamen Vorschlags als Grundlage für die Entwicklung eines weltweiten Verständnisses und einer internationalen Kooperation im Bereich des Datenschutzes und des Schutzes der Privatsphäre, insbesondere im Kontext der internationalen Übertragung personenbezogener Daten, bei der die Rechte und Freiheiten der Individuen geschützt werden müssen.

5. Die Kontaktgruppe soll:

   a. ihre Arbeit mit der Steuerungsgruppe der Konferenz koordinieren und über ihre Vertretung auf Sitzungen internationaler Organisationen entscheiden, sowie

   b. die 32. Internationale Konferenz über ihre Fortschritte informieren, damit die Aufmerksamkeit dauerhaft auf das Thema des vorliegenden Beschlusses gerichtet wird.


Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Schaar
Pressesprecherin
RI'n Heinrich ☎ -916
Zentrale Aufgaben
ROI´n Berger ☎ -911
Koordinierung / Lenkung Öffentlichkeitsarbeit
OAR'in Pawlikowski ☎ -415
Internetredaktion
OAR'in Buske ☎ -317
Verbindungsbüro Berlin
MinR Gronenberg ☎ -950
Leitender Beamter
Dir Bachmeier
Behördlicher Datenschutzbeauftragter
OAR Müller ☎ -315
Referat I
Grundsatzangelegenheiten; nicht-öffentlicher Bereich
MinR Gerhold ☎ -110
Referat II
Arbeits-, Finanz- und Wirtschaftsverwaltung, Rechtswesen, Verteidigung, Zivildienst
MinR Heil ☎ -210
Referat III
Sozial- und Gesundheitswesen, Beschäftigtendatenschutz
RD Raum ☎ -310
Referat IV
Projekte der angewandten Informatik, Telematik
MinR Büttgen ☎ -410
Referat V
Polizei, Nachrichtendienste, Strafrecht, europäische und internationale polizeiliche und justizielle Zusammenarbeit
MinR Heyn ☎ -510
Referat VI
Technologischer Datenschutz, Informationstechnik, Datensicherheit
MinR Landvogt ☎ -610
Referat VII
Europäische und internationale Angelegenheiten, Innere Verwaltung, Auswärtiger Dienst, Stasi-Unterlagen
MinR'n Wuttke-Götz ☎ -710
Referat VIII
Telekommunikations-, Telemedien- und Postdienste
Projektgruppe Elektronische Gesundheitskarte (PG eGK)
MinR Müller J.H. ☎ -810
Referat IX
Informationsfreiheit
MinR Gronenberg ☎ -950
Anschriften:
Bonn: Husarenstr. 30, 53117 Bonn
Berlin: Friedrichstr. 50, 10117 Berlin
Telefon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de
Internet: www.datenschutz.bund.de
Legende:
Aufgaben werden in Bonn wahrgenommen
Aufgaben werden in Berlin wahrgenommen
Stand: 21. Dezember 2010

## Sachregister

Als Fundstelle ist die Nummer des Abschnitts oder des Beitrages angegeben, in dem der Begriff verwendet wird.

**Abkürzungsverzeichnis/Begriffe**

| | |
|---|---|
| AA | Auswärtiges Amt |
| a.a.O | am angegebenen Orte |
| ACTA | Anti-Counterfeiting Trade Agreement |
| ABl. | Amtsblatt der Europäischen Gemeinschaften |
| ABG | Automatisierte und biometriegestützte Grenzkontrolle |
| ABMG | Autobahnmautgesetz |
| Abs. | Absatz |
| AEO | Authorized Economic Operator |
| AEUV | Vertrag über die Arbeitsweise der Europäischen Union |
| AG | Aktiengesellschaft, aber auch: Arbeitsgruppe |
| AG | Amtsgericht |
| AGB | Allgemeine Geschäftsbedingungen |
| ALG II | Arbeitslosengeld II |
| Alt. | Alternative |
| AND | Andere Nachrichtendienste |
| AO | Abgabenordnung |
| AOK | Allgemeine Ortskrankenkasse |
| AOS | Allianz Ortungs Services GmbH |
| ARGE | Arbeitsgemeinschaften nach dem Sozialgesetzbuch II |
| Art. | Artikel |
| ATD | Antiterrordatei |
| ATDG | Antiterrordateigesetz |
| ATM | Asynchronous Transfer Mode |
| AufenthG | Aufenthaltsgesetz |
| AufenthV | Aufenthaltsverordnung |
| AuslG | Ausländergesetz |
| AVV | Allgemeine Verwaltungsvorschrift |
| AWG | Außenwirtschaftsgesetz |
| Az. | Aktenzeichen |
| AZR | Ausländerzentralregister |
| AZRG | Gesetz über das Ausländerzentralregister |
| | |
| BA | Bundesagentur für Arbeit |
| BAFA | Bundesamt für Wirtschaft und Ausfuhrkontrolle |
| BaFin | Bundesanstalt für Finanzdienstleistungsaufsicht |
| BAföG | Bundesausbildungsförderungsgesetz |
| BAG | Bundesamt für Güterverkehr |
| BAköV | Bundesakademie für öffentliche Verwaltung |
| BAMF | Bundesamt für Migration und Flüchtlinge |
| BArchG | Bundesarchivgesetz |

| | |
|---|---|
| BAZ | Bundesamt für den Zivildienst |
| BBG | Bundesbeamtengesetz |
| BBK | Bundesamt für Bevölkerungsschutz und Katastrophenhilfe |
| BCR | Binding Corporate Rules; verbindliche unternehmensinterne Datenschutzregelungen |
| bDSB | behördlicher Datenschutzbeauftragter |
| BDSG | Bundesdatenschutzgesetz |
| BfA | Bundesversicherungsanstalt für Angestellte |
| BFD | Bundesbeauftragter für den Datenschutz |
| BfDI | Bundesbeauftragter für den Datenschutz und die Informationsfreiheit |
| BfD/BA | Beauftragter für den Datenschutz der Bundesanstalt für Arbeit |
| BfV | Bundesamt für Verfassungsschutz |
| BGBl. | Bundesgesetzblatt |
| BISp | Bundesinstitut für Sportwissenschaft |
| BKA | Bundeskriminalamt |
| BKAG | Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten |
| Bluetooth | Standard für die drahtlose Übermitlung von Sprache und Daten im Nahbereich |
| BMAS | Bundesministerium für Arbeit und Soziales |
| BMF | Bundesministerium der Finanzen |
| BMFSFJ | Bundesministerium für Familie, Senioren, Frauen und Jugend |
| BMG | Bundesministerium für Gesundheit |
| BMGS | Bundesministerium für Gesundheit und Soziale Sicherung |
| BMI | Bundesministerium des Innern |
| BMJ | Bundesministerium der Justiz |
| BMVBS | Bundesministerium für Verkehr, Bau- und Stadtentwicklung |
| BMVg | Bundesministerium der Verteidigung |
| BMWi | Bundesministerium für Wirtschaft und Technologie |
| BND | Bundesnachrichtendienst |
| BNDG | Gesetz über den Bundesnachrichtendienst |
| BNetzA | Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen |
| BR | Bundesrat |
| BR-Drs. | Bundesrats-Drucksache |
| BSG | Bundessozialgericht |
| BSH | Bundesamt für Seeschifffahrt und Hydrographie |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BSIG | BSI-Gesetz |
| BStU | Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR |
| BT | Bundestag |
| BT-Drs. | Bundestags-Drucksache |
| BVA | Bundesverwaltungsamt, aber auch: Bundesversicherungsamt |
| BVerfG | Bundesverfassungsgericht |

| | |
|---|---|
| BVerfGE | Entscheidungen des Bundesverfassungsgerichts |
| BVerfSchG | Bundesverfassungsschutzgesetz |
| BVerwG | Bundesverwaltungsgericht |
| BVV | Bundesvermögensverwaltung |
| BZR | Bundeszentralregister |
| BZRG | Bundeszentralregistergesetz |
| BZSt | Bundeszentralamt für Steuern |
| bzw. | beziehungsweise |
| | |
| ca. | circa |
| CC | Common Criteria |
| CD/CD-ROM | Compact Disc – Read Only Memory |
| CIA | Central Intelligence Agency, USA |
| | |
| DB | Deutsche Bahn |
| d. h. | das heißt |
| DDR | Deutsche Demokratische Republik |
| DECT | Digital Enhanced Cordless Telecommunications |
| DHR | Deutsches Hämophilieregister |
| DLZ | Dienstleistungszentrum |
| DNS | Domain Name System |
| Dok. | Dokument |
| DPI | Deep Packet Inspection |
| DPMA | Deutsches Patent- und Markenamt |
| DRM | Digital Rights Management (Digitales Rechte Management) |
| Drs. | Drucksache |
| DRV Bund | Deutsche Rentenversicherung Bund |
| DSL | Digital Subscriber Line |
| DSRV | Datenstelle der Träger der Rentenversicherung |
| DTAG | Deutsche Telekom AG |
| Düsseldorfer Kreis | Koordinierungsgremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich |
| DV/dv | Datenverarbeitung |
| DVB-C | Digital Video Broadcasting-Cable |
| | |
| e.V. | eingetragener Verein |
| E-Commerce | Elektronic Commerce/Elektronischer Handel |
| ED | Erkennungsdienst |
| EDPS | Europäischer Datenschutzbeauftragter |
| EDV | Elektronische Datenverarbeitung |
| EETS/EEMD | Europäischer Elektronischer Mautdienst |

| | |
|---|---|
| EG | Europäische Gemeinschaft(en) |
| eGK | elektronische Gesundheitskarte |
| EG-ZIS | Europäisches Zollinformationssystem |
| EGGVG | Einführungsgesetz zum Gerichtsverfassungsgesetz |
| EHUG | Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister |
| EIS | Europäisches Informationssystem |
| eID | elektronischer Identitätsnachweis, elektronische Identitätsfunktion |
| EJG | Eurojust-Gesetz |
| eKA | elektronische Kriminalakte |
| ELENA | Elektronischer Entgeltnachweis |
| ELStAM | Elektronische LohnSteuerAbzugsMerkmale |
| ELSTER | Elektronische Steuererklärung |
| E-Mail | Electronic Mail |
| EMF | Elektromagnetische Felder |
| EP | Europäisches Parlament |
| EPC | Electronic Product Code — Der EPC besteht aus vier Datenblöcken zur Identifizierung der Version, des Herstellers, der Produktkategorie und des individuellen Gegenstands |
| EPCglobal | EPCglobal Inc. ist ein Joint Venture zwischen EAN International und dem Uniform Code Council (UCC). Die Aufgabe des Nonprofit-Unternehmens liegt in der kommerziellen Vermarktung sowie der Administration des EPC |
| EStA | Register der Entscheidungen in Staatsangehörigkeitsangelegenheiten |
| EstG | Einkommensteuergesetz |
| etc. | ecetera |
| eTIN | Lohnsteuerliches Ordnungsmerkmal |
| EU | Europäische Union |
| EuGH | Europäischer Gerichtshof |
| Eurodac | Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern |
| Europol | Europäisches Polizeiamt |
| EVN | Einzelverbindungsnachweis |
| EWG | Europäische Wirtschaftsgemeinschaft |
| EWR | Europäischer Wirtschaftsraum |
| | |
| f. | folgend |
| FBI | Federal Bureau of Investigation, USA |
| FDZ | Forschungsdatenzentrum |
| ff. | folgende |
| FH Bund | Fachhochschule des Bundes für öffentliche Verwaltung |
| FIFA | Fédération Internationale de Football Association |
| FKS | Finanzkontrolle Schwarzarbeit |
| FTC | Federal Trade Commission |
| FVG | Finanzverwaltungsgesetz |

| | |
|---|---|
| G.10 | Artikel 10 Gesetz |
| GASIM | Gemeinsames Analyse- und Strategiezentrum Illegale Migration |
| GBA | Generalbundesanwalt beim Bundesgerichtshof |
| gem. | gemäß |
| GG | Grundgesetz |
| ggf. | gegebenenfalls |
| GGO | Gemeinsame Geschäftsordnung der Bundesministerien |
| GIZ | Internetzentrum |
| GJVollz-E | Gesetzentwurf zur Regelung des Jugendstrafvollzugs |
| GKI | Gemeinsame Kontrollinstanz |
| GKV | Gesetzliche Krankenversicherung |
| GKV-WSG | Gesetz zur Stärkung des Wettbewerbs in der Gesetzlichen Krankenversicherung |
| GmbH | Gesellschaft mit beschränkter Haftung |
| GMBl | Gemeinsames Ministerialblatt |
| GMG | Gesetz zur Modernisierung der gesetzlichen Krankenversicherung |
| GPEN | Global Privacy Enforcement Network |
| GPS | Global Positioning System |
| GRCh | EU-Grundrechtecharta |
| GS1 | Global Standards One |
| GSM | Global System for Mobile Communications |
| GTAZ | Gemeinsames Terrorismusabwehrzentrum |
| GwG | Geldwäschegesetz |
| | |
| HKP | häusliche Krankenpflege |
| HPC | Health Professional Card |
| HSM | Hardware Security Modul |
| HTTP | Hypertext Transfer Protocol |
| HVBG | Hauptverband der gewerblichen Berufsgenossenschaften |
| | |
| IATA | International Air Transport Association |
| i. d. F. | in der Fassung |
| i. S. d. | im Sinne des (der) |
| i. S. v. | im Sinne von |
| i. V. m. | in Verbindung mit |
| ICAO | International Civil Aviation Organization |
| ICHEIC | International Commission on Holocaust Era Insurance Claims |
| IFG | Informationsfreiheitsgesetz |
| IFOS-Bund | Interaktives Fortbildungssystem für die Bundesverwaltung |
| IHK | Industrie- und Handelskammer |
| IKPO | Internationale Kriminalpolizeiliche Organisation |
| IKT | Informations- und Kommunikationstechnologie |

| | |
|---|---|
| ILO | International Labour Organization |
| IMI | Binnenmarktinformationssystem |
| IMK | Ständige Konferenz der Innenminister und -senatoren der Länder |
| IMSI | International Mobile Subscriber Identity |
| INPOL | Informationssystem der Polizei |
| InsO | Insolvenzordnung |
| IntV | Integrationskursverordnung |
| IP | Internet Protocol |
| IPR | Internationales Privatrecht |
| ISDN | Integrated Services Digital Network |
| ISO | International Organization for Standardization |
| IT | Informationstechnik |
| IVBB | Informationsverbund Berlin-Bonn |
| | |
| JI-Rat | Rat der Innen- und Justizminister der Europäischen Union |
| | |
| KBA | Kraftfahrt-Bundesamt |
| KFU | Krebsfrüherkennungsrichtlinien |
| Kfz | Kraftfahrzeug |
| KIWI | Kindergeld-Windows-Implementierung |
| KOM | Europäische Kommission |
| KWG | Kreditwesengesetz |
| | |
| LfD | Landesbeauftragter für den Datenschutz |
| LfV | Landesamt für Verfassungsschutz |
| lit. | litera (=Buchstabe) |
| LKA/LKÄ | Landeskriminalamt/Landeskriminalämter |
| LuftSiG | Gesetz zur Neuregelung von Luftsicherheitsaufgaben (Luftsicherheitsgesetz) |
| | |
| m. E. | meines Erachtens |
| MAD | Militärischer Abschirmdienst |
| MAK | Mindestanforderungen an das Kreditgeschäft der Kreditinstitute |
| MDK | Medizinischer Dienst der Krankenversicherung |
| MfS | Ministerium für Staatssicherheit |
| MI6 | Military Intelligence, Section 6 |
| MRI | Max-Rubner-Institut |
| MRRG | Melderechtsrahmengesetz |
| MSU | Mail Sampling Unit |
| MVDS | Multifunktionaler Verdienstdatensatz |
| MZG | Mikrozensusgesetz |

| | |
|---|---|
| NADIS | Nachrichtendienstliches Informationssystem |
| NADIS-WN | Narichtendienstliches Informationssystem – Wissensnetz |
| NATO | North Atlantic Treaty Organization |
| NEMONIT | Nationales Ernährungsmonitoring |
| NGN | Next Generation Network |
| NJW | Neue Juristische Wochenschrift |
| nPA | elektronischer Personalausweis, neuer Personalausweis |
| Nr. | Nummer |
| NSDAP | Nationalsozialistische Deutsche Arbeiterpartei |
| NTS | Nato-Truppenstatut |
| NVSII | Nationale Verzehrstudie II |
| NWR | Nationales Waffenregister |
| | |
| o. a. | oben aufgeführt |
| o. g. | oben genannt |
| OECD | Organisation für wirtschaftliche Zusammenarbeit und Entwicklung |
| OFD | Oberfinanzdirektion |
| OK | Organisierte Kriminalität, aber auch: Organisationskomitee |
| OLAF | Europäisches Amt für Betrugsbekämpfung |
| OVG | Oberverwaltungsgericht |
| | |
| PassG | Passgesetz |
| PAVOS | Polizeiliches Auskunfts- und Vorgangsbearbeitungssystem (beim BGS) |
| PbD | Privacy by Design |
| PC | Personalcomputer |
| PDA | Personal Digital Assistant |
| PEI | Paul-Ehrlich-Institut |
| PersauswG | Personalausweisgesetz |
| PIA | Privacy Impact Assessment |
| PIN | Persönliche Identifikationsnummer |
| PKGr | Parlamentarisches Kontrollgremium |
| PNR | Passenger Name Record |
| Protection Profile | Schutzprofil |
| | |
| Ratsdok. | Ratskokument (EU) |
| RatSWD | Rat für Sozial- und Wirtschaftsdaten |
| Rdn. | Randnummer |
| Reha | Rehabilitation |
| REHA-Maßnahmen | Rehabilitationsmaßnahme |
| RFID | Radio Frequency Identification – Transpondertechnik für die berührungslose Erkennung von Objekten |

| | |
|---|---|
| RFID-Chip | Radio Frequency Identification-Chip (Funkchip) |
| RFV | Registratur Fachverfahren |
| RKI | Robert-Koch-Institut |
| RSAV | Risikostrukturausgleichsverordnung |
| RVOrgG | Organisationsreform in der gesetzlichen Rentenversicherung |
| | |
| S. | Seite |
| s. | siehe |
| s. o. | siehe oben |
| s. u. | siehe unten |
| SCHUFA | Schutzgemeinschaft für allgemeine Kreditsicherung |
| SchwarzArbG | Schwarzarbeitsbekämpfungsgesetz |
| SDÜ | Schengener Durchführungsübereinkommen |
| SG | Soldatengesetz |
| SGB | Sozialgesetzbuch |
| SGB I | Sozialgesetzbuch Erstes Buch (Allgemeiner Teil) |
| SGB II | Sozialgesetzbuch Zweites Buch (Grundsicherung für Arbeitssuchende) |
| SGB III | Sozialgesetzbuch Drittes Buch (Arbeitsförderung) |
| SGB IV | Sozialgesetzbuch Viertes Buch (Gemeinsame Vorschriften für die Sozialversicherung) |
| SGB V | Sozialgesetzbuch Fünftes Buch (Gesetzliche Krankenversicherung) |
| SGB VI | Sozialgesetzbuch Sechstes Buch (Gesetzliche Rentenversicherung) |
| SGB VII | Sozialgesetzbuch Siebentes Buch (Gesetzliche Unfallversicherung) |
| SGB VIII | Sozialgesetzbuch Achtes Buch (Kinder- und Jugendhilfe) |
| SGB IX | Sozialgesetzbuch Neuntes Buch (Rehabilitation und Teilhabe behinderter Menschen) |
| SGB X | Sozialgesetzbuch Zehntes Buch (Sozialverwaltungsverfahren und Sozialdatenschutz) |
| SGB XI | Sozialgesetzbuch Elftes Buch (soziale Pflegeversicherung) |
| SGB XII | Sozialgesetzbuch Zwölftes Buch (Sozialhilfe) |
| SigG | Signaturgesetz |
| SIM | Subscriber Identity Module |
| SiMKo2 | Sichere Mobile Kommunikation |
| SMS | Short Message Service |
| SNS | Sichere Netzübergreifende Sprachkommunikation |
| SOG | Gesetz über öffentliche Sicherheit und Ordnung |
| sog. | so genannt |
| SPD | Sozialdemokratische Partei Deutschlands |
| STADA | Staatsangehörigkeitsdatei |
| StAG | Staatsangehörigkeitsgesetz |
| Stasi | Staatssicherheitsdienst der ehemaligen DDR |
| StDAV | Steuerdaten-Abruf-Verordnung |
| StDÜV | Steuerdatenübermittlungsverordnung |
| Steuer-ID | Steuer-Identitätsnummer |
| StGB | Strafgesetzbuch |

| | |
|---|---|
| StPO | Strafprozessordnung |
| StUG | Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz) |
| StVBG | Steuerverkürzungsbekämpfungsgesetz |
| StVergAbG | Steuervergünstigungsabbaugesetz |
| StVG | Straßenverkehrsgesetz |
| StVollzG | Strafvollzugsgesetz |
| SDDSG | Suchdienstedatenschutzgesetz |
| SÜFV | Sicherheitsüberprüfungsfeststellungsverordnung |
| SÜG | Sicherheitsüberprüfungsgesetz |
| SWIFT | Society for Worldwide Interbank Financial Telecommunication |
| | |
| TAB | Büro für Technikfolgenabschätzung beim Deutschen Bundestag |
| TAL | Teilnehmeranschlussleitung |
| TAN | Transaktionsnummer |
| TB | Tätigkeitsbericht |
| TBEG | Terrorismusbekämpfungsgesetz |
| TBG | Terrorismusbekämpfungsgesetz |
| TFG | Transfusionsgesetz |
| TFTP | Terrorist Finance Tracking Program |
| THW | Bundesanstalt Technisches Hilfswerk |
| TK | Telekommunikation |
| TKG | Telekommunikationsgesetz |
| TKÜ | Telekommunikationsüberwachung |
| TMG | Telemediengesetz |
| TOP | Tagesordnungspunkt |
| TR | Technische Richtlinie |
| | |
| u. a. | unter anderem |
| u. ä. | und ähnliches |
| u. U. | unter Umständen |
| UIG | Umweltinformationsgesetz |
| ULD | Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein |
| UrhG | Urheberrechtsgesetz |
| URL | Uniform Resource Locator |
| US | United States |
| USA | United States of America |
| UStG | Umsatzsteuergesetz |
| usw. | und so weiter |
| | |
| VAM | Virtueller Arbeitsmarkt |
| VBM | vorläufiges Bearbeitungsmerkmal |

| | |
|---|---|
| VdAK | Verband der Angestellten-Krankenkassen |
| VDR | Verband Deutscher Rentenversicherungsträger |
| VDS | Vorratsdatenspeicherung |
| VG | Verwaltungsgericht |
| vgl. | vergleiche |
| VN | Vereinte Nationen |
| VoIP | Voice over IP |
| VPN | Virtual Private Network (dt. virtuelles privates Netz) |
| vpS | Vorbeugender personeller Sabotageschutz |
| VS | Verschlusssache |
| WADA | Welt-Anti-Doping-Agentur |
| WiMax | Wordwide Interoperability for Microwave Access Standard gemäß IEEE 802.16a für lokale Funknetze |
| WLAN | Wireless Local Area Network |
| WM | Weltmeisterschaft |
| WP | Working Paper |
| WPK | Wirtschaftsprüferkammer |
| WPO | Wirtschaftsprüferordnung |
| WPPJ | Working Party Police and Justice (Arbeitsgruppe Polizei und Justiz) |
| WPV | Versorgungswerk der Wirtschaftsprüfer |
| WSA | Wasser- und Schifffahrtsamt |
| www | World wide web |
| XML | Extensible Markup Language |
| z. B. | zum Beispiel |
| z. T. | zum Teil |
| ZAG | Zentren für Arbeit und Grundsicherung |
| ZAUBER | Abrufverfahren |
| ZDG | Zivildienstgesetz |
| ZensG 2011 | Zensusgesetz 2011 |
| ZFdG | Zollfahndungsdienstgesetz |
| ZFER | Zentrales Fahrerlaubnisregister |
| ZIS | Zollinformationssystem |
| ZIVIT | Zentrum für Informationsverarbeitung und Informationstechnik |
| ZKA | Zollkriminalamt |
| ZORA | Zukunftsorientierte Retailanwendung |
| ZPO | Zivilprozessordnung |
| ZSS | Zentrale Speicherstelle |
| ZStV | Zentrales Staatsanwaltschaftliches Verfahrensregister |

**Übersicht Alle Tätigkeitsberichte**

| Tätigkeitsbericht | Berichtszeitraum | Bundestags-Drucksachennummer |
|---|---|---|
| 1. | 1978 | 8/2460 |
| 2. | 1979 | 8/3570 |
| 3. | 1980 | 9/93 |
| 4. | 1981 | 9/1243 |
| 5. | 1982 | 9/2386 |
| 6. | 1983 | 10/877 |
| 7. | 1984 | 10/2777 |
| 8. | 1985 | 10/4690 |
| 9. | 1986 | 10/6816 |
| 10. | 1987 | 11/1693 |
| 11. | 1988 | 11/3932 |
| 12. | 1989 | 11/6458 |
| 13. | 1990 | 12/553 |
| 14. | 1991 – 1992 | 12/4805 |
| 15. | 1993 – 1994 | 13/1150 |
| 16. | 1995 – 1996 | 13/7500 |
| 17. | 1997 – 1998 | 14/850 |
| 18. | 1999 – 2000 | 14/5555 |
| 19. | 2001 – 2002 | 15/888 |
| 20. | 2003 – 2004 | 15/5252 |
| 21. | 2005 – 2006 | 16/4950 |
| 22. | 2007 – 2008 | 16/12600 |

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

**Der Bundesbeauftragte für den Datenschutz**
**und die Informationsfreiheit**
Husarenstraße 30
D-53117 Bonn

Tel. +49 (0) 228 997799-0
Fax +49 (0) 228 997799-550
E-Mail: poststelle@bfdi.bund.de
Internet: www.bfdi.bund.de

Bonn 2011

Dieser Bericht ist als Bundestagsdrucksache 17/5200 erschienen.

Druck: Druckpartner Moser
Druck + Verlag GmbH
Römerkanal 52-54
53359 Rheinbach